

tomasof@privacyinternational.org

By email only

Brussels, 23 January 2019

Ref: GG-439-2018

Subject: Letter from 19 November 2018 on Romanian DPA Investigation

Dear civil society privacy organisations' Members,

Thank you very much for the letter you sent me on 19 November 2018 regarding the request for information submitted by the Romanian Data Protection Authority to the RISE project, which I have carefully read.

As foreseen in article 58 GDPR, each Supervisory Authority (SA) has the power to request any information from a controller or from a processor in the context of a given processing operation that is necessary for the performance of its tasks. The fundamental right to the protection of personal data that such power aims to protect, however, has to be balanced against the protection of other equally important fundamental rights (such as the right to freedom of expression and information). It goes without saying that the protection of journalistic sources is a cornerstone of the freedom of the press.

Furthermore, such powers must take into consideration the requirements foreseen in article 85 GDPR, which mandate a legal reconciliation of both fundamental rights, including in cases where processing for journalistic purposes is involved. Even though article 85 leaves such task to Member States, it is clear that such reconciliation must always be done in respect of chapter VII of the GDPR and of the applicable jurisprudence of the CJEU and the ECtHR.

Moreover, it is essential to add that such powers should be exercised in a proportionate manner and based on an individual assessment of each case. The same reasoning is applicable to any fines issued by an SA under the GDPR: they need to be imposed casuistically and be, not only effective and dissuasive, but also proportionate to the demonstrated infringement.

I would like to underline that the European Data Protection Board (EDPB) does not have the same competences, tasks and powers as national supervisory authorities. The assessment of alleged infringements of the GDPR in first instance falls within the competence of the responsible and independent Supervisory Authorities of each Member State, either by themselves or in cooperation with other SAs. A judicial remedy will always be available in accordance with article 78(1) GDPR.

Yours sincerely,


Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

Letters



European Union Agency for Cybersecurity
Ethnikis Antisaseos 72 & Agamemnonos 14,
Chalandri 15231, Attiki
Greece

Sent by e-mail only

Brussels, 18 November 2021

Ref: OUT2021-00157

Dear Mr. Lepassaar,

Thank you for your response to our letter regarding the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and your invitation to work together on the establishment of guidance for cloud service providers that would explain to them how to best use the EUCS to meet the cybersecurity requirements of the GDPR. This proposition will be discussed thoroughly among the data protection authorities and we will come back to you on this topic later on.

However, for this work to be fruitful, it is necessary that the final certification Scheme is consistent with the obligations laid down in the GDPR and facilitates the compliance with the GDPR of cloud service providers (CSP) and their clients.

In this respect, the Schrems II judgement of the CJEU¹ is a key issue that shall be addressed by CSPs in order to help their clients with the compliance of the processing that they host. This compliance can be reached in various ways, as the EDPB explained in its Recommendations on supplementary measures², including with certain approaches to encryption and key management.

Therefore, the EDPB considers that at least an assurance level of the EUCS should include appropriate specific criteria to ensure protection against threats represented by access from authorities not subject to EU legislation and not offering a level of protection of personal data that is essentially equivalent to that guaranteed by the GDPR and recalled by the CJEU.

Offering an assurance level of the EUCS with strong guarantee that the cloud service provider is not subject to foreign access incompatible with the GDPR would facilitate the compliance of processing activities relying on cloud services certified with this level of assurance. Failing to do so would be a missed opportunity to foster security and compliance across Europe.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0311>

² https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

We believe that especially such criteria will help ensuring security not only for personal data, but for all kinds of information that needs protection against the abovementioned threats.

We are ready to assist you already in the formulation of these criteria and are looking forward to continue our fruitful collaboration.

Yours sincerely,



Andrea Jelinek

European Commission

22 January 2021
Ref: OUT2021-0004

Dear Commissioner Schinas,
Dear Commissioner Johansson,
Dear Commissioner Reynders,

The European Data Protection Board (EDPB) took note of the Commission report on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, which was published on 24 July 2020.¹

As main conclusion, the Commission considers that assessment of the first two years of application of the Directive is overall positive and takes the view that no amendments to the PNR Directive should be proposed at this stage. The Commission also considers that some issues like a possible extension of the Directive's scope shall be further assessed. Furthermore, before deciding whether to propose a revision the Commission wishes to take into account the results of the on-going evaluation of the Advance Passenger Information Directive as well as the outcome of the preliminary ruling requests currently before the Court of Justice.²

The EDPB wishes to recall that the European data protection authorities already identified a need for amending the PNR Directive after analysing the reasoning of the CJEU on the envisaged PNR agreement with Canada³. This was put forward to the Commission in a letter of the former Working Party 29 (WP29) on 11 April 2018.⁴ In the view of the WP29, the Court's Opinion, though not having a formal legal effect on other acts of the Union, highlighted deficiencies that could equally be found in other PNR instruments. Regarding the PNR directive, the WP29 in particular pointed out that the indiscriminate and long-term retention of PNR data and access to them after passengers have been cleared in security and border

¹ COM(2020) 305 final.

² Request for a preliminary ruling in Case C-817/19 Ligue des droits humains, OJ C 36, 3.2.2020, p. 16-17 (pending); request for preliminary ruling in joined Cases C-148/20, C-149/20 and C-150/20 Deutsche Lufthansa, OJ C 279/21, 24.08.2020, p. 21-22 (pending); request for preliminary ruling in joined Cases C-215/20 and C220/20, not yet published (pending).

³ CJEU Opinion 1/15 (Grand Chamber) of 26 July 2017.

⁴ https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51023.

control checks are not in compliance with the Opinion of the CJEU. While the processing, retention and transfer of PNR data is generally subject to stricter rules in the EU PNR directive than in the envisaged PNR agreement with Canada, the WP29 considered in 2018 that the EU PNR directive is at least partly not in compliance with the requirements expressed by the CJEU in its opinion. The EDPB upholds the former position of the WP29 and reiterates its call upon the European Commission to take action in order to ensure compliance with the CJEU's opinion regarding both PNR agreements with the US and Australia as well as regarding the PNR directive.

In the view of the EDPB, the review report does not explicitly confirm, nor substantiate in a comprehensive manner, the necessity and proportionality of the indiscriminate collection and processing of PNR data for the purposes of the PNR Directive, but rather raises even more doubts.

In this context, and in relation to the necessity principle and the retention and use of PNR data, the EDPB recalls that the CJEU in its opinion on the envisaged EU-Canada PNR agreement considered that "*the average lifespan of international serious crime networks and the duration and complexity of investigations relating to those networks, do not justify the continued storage of the PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with combating terrorism and serious transnational crime (see, by analogy, judgment of 21 December 2016, Tele2 Sverige and Watson and Others, C-203/15 and C-698/15, EU:C:2016:970, paragraph 119).*"⁵ While this reasoning applied in the case of data retention and processing after departing a third country, the EDPB considers that the conclusion of the CJEU and the link between the retention of PNR data and the combatting of serious transnational crime remains relevant within the scope of the EU PNR Directive review and necessity assessment.

Furthermore, the EDPB would like to stress that the CJEU also recently held in *La Quadrature du Net and others*, that "*legislation requiring the retention of personal data must always meet objective criteria that establish a connection between the data retained and the objective pursued*"⁶. In the same context, in *Privacy International*, it also held that the legislator "*must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue*"⁷. In light of this recent case-law, the EDPB considers that the review of the EU PNR Directive must rely on

⁵ CJEU Opinion 1/15 (Grand Chamber) of 26 July 2017, § 205.

⁶ CJEU Judgement in joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, § 133.

⁷ CJEU Judgement in case C-623/17, *Privacy International*, § 78.

solid and evidence-based elements able to demonstrate the connection between the PNR data retained and the objective pursued.

The Commission points out the Member States' assumption that the different means of processing of PNR data available to them (i.e. real time, reactive and proactive) have already delivered tangible results in the fight against terrorism and crime. Thirteen case studies are presented as qualitative evidence in the accompanying Staff Working Document.⁸ However, the specifics and detailed circumstances of these case studies have not been made available, which therefore cannot be considered as sufficient elements able to substantiate in a general manner the necessity and proportionality of the processing under the EU PNR Directive.

Remarkably, in at least one of those case studies, the processing of PNR merely led to a time advantage. The fugitive, convicted to a six-year prison sentence for drug-related offences who was wanted by the authorities, would have been subject to a Schengen Information System (SIS) check in border controls as a traveler from a third country anyway. This check would have resulted in the identification, since a wanted fugitive is subject to specific alert within SIS. Whether PNR data were necessary at all to identify this person, is at least questionable, and may not allow to draw general conclusions as to the necessity of a general retention of PNR data. In addition, the upcoming implementation of the European Travel Information and Authorisation System (ETIAS), applicable to travelers exempted from visa requirements, would render this case even less relevant, as the individual coming from a non-EU country would be identified prior to entering the EU, at the time of the request for travel authorisation.

Even if not being exhaustive, the small number of case studies has to be seen in the light of the total amount of processing, which is processing of mass data. The statistics gathered by the Commission for 2019 indicate that 0.59% of all passengers whose data have been collected have been identified through automated processing as requiring further examination. An even smaller fraction of 0.11% was transmitted to competent authorities.⁹ In the view of the Commission this means that, overall, PNR systems deliver targeted results which limit the degree of interference with the rights to privacy and the protection of personal data of the vast majority of bona fide travelers. However, there is still a gap of 0.48% of passengers who were subject to further verification measures and 0.11% who were subject to further measures of the competent authorities.

⁸ SWD(2020) 128 final.

⁹ SWD(2020) 128 final, p. 28.

What might seem a very small amount of passengers, looks much larger when transferring it into total numbers of persons, for example with figures from 2018 as provided by Eurostat. Though the Eurostat figures may also include flights for which PNR data may not have been systematically collected, the EDPB considers these figures as relevant to draw conclusions in terms of scale and volume¹⁰. In 2018, 1.1 billion passengers travelled by air in the European Union, 16 % of those in national transport, the rest in intra-EU and extra-EU flights.¹¹ This would amount to 924 million passengers being subject to the collection of PNR data. With 0,59% of technical hits there would have been 5.451.600 persons subject to further processing in one year, 4.435.200 of them would have been sorted out and still, data of 1.016.400 persons would have been transmitted to competent authorities for further measures.

The great amount of persons concerned compared to the little evidence for the usefulness of PNR data given in the few case studies up to now, raises serious doubts towards the proportionality of such mass data processing.

In any case, the high number of persons sorted out in manual verification after technical hits shows an issue with data quality. This is notably due to the fact that PNR data are collected by carriers for a different purpose. For example, PNR data do not necessarily contain birth dates of air passengers. Therefore, real time comparison with EU information systems such as the Schengen Information System will almost inevitably produce a number of false or at least unverifiable matches. All those matches would then need to be further processed for manual verification, which may often lead to a dead end because of the missing birth date. The same issue may arise with reactive processing.

Having considered the Commission review report of the EU PNR Directive, and taking into account the latest CJEU case law, the EDPB takes the view that the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in the Directive, as referred to in its Article 19, is not sufficiently substantiated and demonstrated. While the EDPB would very much welcome any further detailed assessment and communication in this regard, it reiterates in the meantime its call on the European Commission to take action, in due time taking into account the related CJEU cases currently pending, in order to ensure compliance of all EU PNR instruments, including the EU PNR

¹⁰ On the basis of the information available and the practices of Member States for the collection of PNR data for intra-EU flights, it seems that the proportion of flights from the Eurostat figures which would not be subject to PNR data collection remains marginal.

¹¹ See Eurostat statistics under <https://ec.europa.eu/eurostat/documents/2995521/10265946/7-06122019-AP-EN.PDF/8f2c9d16-c1c4-0e1f-7a66-47ce411faef7>.

Directive, with EU law and case-law. The EDPB stands ready to engage in further discussions and provide input to the Commission in this task.

Yours sincerely,



Andrea Jelinek

Sophie in't Veld MEP
European Parliament
Rue Wiertz 60
B-1047 Brussels
Belgium

25 January 2021

Ref: OUT2021-0005

Dear Ms in 't Veld,

I would like to thank you for your letter of 14 September 2020 regarding the Commission's report on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, which was published on 24 July 2020. The EDPB also took note of the accompanying Staff Working Document and the case studies given to prove that the Directive is contributing positively to its key objectives.

As main conclusion, the Commission considers that the assessment of the first two years of application of the Directive is overall positive and takes the view that no amendments to the PNR Directive should be proposed at this stage. The Commission also considers that some issues like a possible extension of the Directive's scope shall be further assessed. Furthermore, before deciding whether to propose a revision, the Commission wishes to take into account the results of the on-going evaluation of the Advance Passenger Information Directive as well as the outcome of the preliminary ruling requests currently before the Court of Justice of the European Union.

The Commission's conclusion clearly contradicts the opinion which the European data protection authorities had already put forward on 11 April 2018 in a letter of the former Working Party 29 (WP29) to the Commission¹. The letter was an urge to react on the opinion of the CJEU on the envisaged PNR agreement with Canada. In the view of the WP29, the Court's Opinion, though not having a formal legal effect on other acts of the Union, highlighted deficiencies that could equally be found in other EU PNR instruments. While the processing, retention and transfer of PNR data is generally subject to stricter rules in the EU PNR Directive than in the envisaged PNR agreement with Canada, the WP29 considered in 2018 that the EU PNR Directive is at least partly not in compliance with the requirements expressed by the CJEU in its opinion. The EDPB upholds the former position of the WP29. Therefore, the EDPB has already reiterated its call on the European Commission to take action, in due time taking into account the related CJEU cases currently pending, in order to ensure compliance of all EU PNR

¹ https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51023.

instruments, including the EU PNR Directive, with EU law and case-law in a letter of the Chair to the European Commission.²

Your questions regarding the PNR evaluation report get to the heart of the matter and reflect concerns which the EDPB also continues to share. More specifically, you raised questions concerning the big discrepancy between the total number of persons being subject to the processing of PNR data in comparison to technical hits and verified hits as well as the small number of case studies provided as qualitative evidence.

The EDPB has raised similar questions and concerns in its letter to the Commission. Having considered the Commission review report of the EU PNR Directive, and taking into account the latest CJEU case law (La Quadrature du Net and others), the EDPB takes the view that the necessity and proportionality of collecting and processing PNR data for each of the purposes set out in the Directive, as referred to in its Article 19, is not sufficiently substantiated and demonstrated.

Another question relates to the recommendations towards the Commission to ensure that fundamental rights standards are fully complied with, whether the EDPB will provide advice to the European Court of Justice (CJEU) in this case and whether there will be a formal reaction to the review report. The latter has been addressed by the above-mentioned letter of the Chair to the European Commission.

Regarding the cases pending at the CJEU, to date, the Court has not asked the EDPB to provide advice in pending cases regarding PNR. The EDPB is not party to these pending procedures and can only submit its views to these cases if formally called upon by the Court. However, the EDPB's letters to the Commission and previous positions expressed are all publicly available.

With regard to recommendable actions to ensure that fundamental rights standards are fully complied with, the EDPB has already and repeatedly recommended to review all PNR instruments and bring them into compliance with EU law and case law. This has to be the first step to be initiated by the European Commission which should then ensure that Member States respect the requirements set by those updated instruments.

Yours sincerely,



Andrea Jelinek

² EDPB letter to the European Commission of 22 January 2021, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-letter-european-commission-commission-report-review_en

Moritz Körner MEP
European Parliament
Rue Wiertz 60
B-1047 Brussels
Belgium

9 July 2020

Ref: OUT2020-0069

RE: Concerns raised with the European Data Protection Board in relation to Airbnb

Dear Mr Körner

I refer to your letter dated 24 January 2020 outlining your concerns in relation to reports that the Airbnb used software to screen personal data of individuals to analyse the online “personality” of users and whether this screening was compatible with the General Data Protection Regulation (GDPR).

Thank you very much for bringing this important topic to our attention. It is likely that any complaints raised in relation to this processing will be cross-border in nature, and therefore the One-Stop-Shop mechanism of the GDPR will apply. This mechanism ensures that the lead supervisory authority responsible for investigating the complaints against Airbnb cooperates and considers the input of any concerned supervisory authorities.

The Irish Data Protection Commission is the lead supervisory authority for Airbnb. I understand that it has already been in contact with you regarding the concerns you raised in your letter, and provided you with additional information in relation to its engagement with Airbnb in relation to this issue.

The EDPB is not able to comment on the activities of national supervisory authorities. In addition, we do not have the competence to launch investigations, as this competence lies exclusively with national supervisory authorities. However, we are confident that the GDPR and EDPB cooperation mechanisms will enable the national supervisory authorities to work together regarding these cases and ensure the uniform application of the GDPR in the EEA.

Yours sincerely,



Andrea Jelinek

Opinion of the Board (Art. 64)



Opinion 04/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Norican Group

Adopted on 18 March 2022

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Norican Group was reviewed by the DK SA as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Norican Group requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 18/01/2022. The decision on the completeness of the file was taken on 1/02/2022.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Norican Group covers the processing of personal data carried out by Norican Group entities bound by the BCR, when they act as controllers or as processors on behalf of another controller of the Group⁷.
4. Concerned data subjects include, job candidates, Norican Group's employees, customers (end-users) and employees of customers (businesses), suppliers, partner firms and other business relations of Norican Group⁸.
5. The draft BCR-C of Norican Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of Norican Group contains all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement regarding Binding Corporate Rules⁹, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Norican Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18¹⁰, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ Norican Group BCR-C, section 2.3 (Geographical scope) and 13.1.

⁸ Norican Group BCR-C, section 2.4.1 (General description of the data flows) and Appendix 1, section 4.

⁹ Referred as "Binding Corporate Rules Agreement" in Annex 2, Appendix 2.

¹⁰ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU¹¹.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

¹¹ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 06/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of Kumon Group

Adopted on 16 February 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.
- (2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.
- (3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors, (hereinafter "BCR-P"), including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Kumon Group were reviewed by the Spanish Supervisory Authority ("Agencia Española de Protección de Datos") as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-P of Kumon Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 7 December 2020. The decision on the completeness of the file was taken on 22 December 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-P of Kumon Group cover the collection, transfer between, and all other processing by the Kumon Group Companies⁶ of personal data originating in the EEA, when the Kumon Group Companies act as data processors for a third party.
4. Concerned data subjects include franchise instructors, students studying (or interested in studying) in the Kumon program and students' parents.
5. The draft BCR-P of Kumon Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Kumon Group draft BCRs-P contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Kumon Group's Intercompany Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs-P of Kumon Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the ES Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the ES Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the ES Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁶ As listed in Appendix I of the BCR-P of Kumon Group.

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 07/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Kumon Group

Adopted on 16 February 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Kumon Group were reviewed by the Spanish Supervisory Authority ("Agencia Española de Protección de Datos") as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Kumon Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 7 December 2020. The decision on the completeness of the file was taken on 22 December 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Kumon Group covers the collection, transfer between, and all other processing by the Kumon Group Companies⁶ of personal data originating in the EEA.
4. Concerned data subjects include franchise instructors, students studying (or interested in studying) in the Kumon program, students' parents and employees.
5. The draft BCR-C of Kumon Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Kumon Group draft BCRs-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Kumon Intra Group Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs-C of Kumon Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁶ As listed in Appendix I of BCR-C of Kumon Group.

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 8/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Processor Binding Corporate Rules of Luxoft Group

Adopted on 16 February 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors, (hereinafter "BCR-P"), including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Luxoft Group were reviewed by the Baden-Wurttemberg Supervisory Authority as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-P of Luxoft Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 14 October 2020. The decision on the completeness of the file was taken on 22 December 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-P of Luxoft Group cover direct or indirect intra-group transfers of personal data from the EEA between members of the Luxoft Group and the subsequent processing of such data as a processor by a member of Luxoft Group outside the EEA.
4. Concerned data subjects include employees of Luxoft Group, including managers, directors, shareholders, affiliates, officers, trainees, interns, representatives and private entrepreneurs; job applicants; visitors (i.e. guests, directors, members of Board of Directors, members of top manager's families or other important partners); and existing and potential end customers or clients of Luxoft.
5. The draft BCR-P of Luxoft Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Luxoft Group draft BCRs-P contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake to be bound by the BCRs, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs -P of Luxoft Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Baden-Wurttemberg Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Baden-Wurttemberg Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Baden-Wurttemberg Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁶, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁶ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 09/2021 on the draft decision of the Baden-Wurttemberg Supervisory Authority regarding the Controller Binding Corporate Rules of Luxoft Group

Adopted on 16 February 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Luxoft Group were reviewed by Baden-Wurttemberg Supervisory Authority as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Luxoft Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 14 October 2020. The decision on the completeness of the file was taken on 22 December 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Luxoft Group covers direct or indirect intra-group transfers of personal data of members of Luxoft Group from EEA, including any such personal data that originated from the EEA and is currently processed by a member of Luxoft Group outside the EEA.
4. Concerned data subjects include employees of all Luxoft Group, such as managers, officers, trainees, interns, representatives and private entrepreneurs, job applicants, partners (i.e. potential customers, end customers, suppliers, business partners, investors and other parties) and visitors (i.e. guests, directors, members of the Board of Directors, members of top manager's families or other important partners).
5. The draft BCR-C of Luxoft Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Luxoft Group draft BCRs-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by taking the steps to be bound by the BCRs, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs-C of Luxoft Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁶, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁶ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 70.1.s)

Art. 70.1.s

**Opinion 14/2021 regarding the European Commission Draft
Implementing Decision pursuant to Regulation (EU)
2016/679 on the adequate protection of personal data in
the United Kingdom**

Adopted on 13 April 2021

CONTENTS

1.	EXECUTIVE SUMMARY.....	4
1.1.	Areas of convergence	5
1.2.	Challenges	5
1.2.1.	General	5
1.2.2.	General data protection aspects	6
1.2.3.	On the access by public authorities to data transferred to the UK	8
1.3.	Conclusion	10
2.	INTRODUCTION	10
2.1.	UK data protection framework.....	10
2.2.	Scope of the EDPB's assessment	11
2.3.	General comments and concerns.....	12
2.3.1.	International commitments entered into by the UK	13
2.3.2.	Possible future divergence of the UK Data Protection Framework	13
3.	GENERAL DATA PROTECTION ASPECTS	15
3.1.	Content principles	15
3.1.1.	Rights of access, rectification, erasure and objection	15
3.1.2.	Restrictions on onward transfers	20
3.2.	Procedural and Enforcement Mechanisms	27
3.2.1	Competent Independent Supervisory Authority	27
3.2.2.	Existence of a data protection system ensuring a good level of compliance	28
3.2.3.	The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms	28
4.	ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EU BY PUBLIC AUTHORITIES IN THE UK.....	29
4.1.	Access and use by UK public authorities for criminal law enforcement purposes	29
4.1.1.	Legal bases and applicable limitations/safeguards	29
4.1.1.1.	The use of consent	29
4.1.1.2.	Search warrants and production orders.....	29
4.1.1.3.	Investigatory powers for law enforcement purposes	30
4.1.2.	Further use of the information collected for law enforcement purposes (recitals 140-154)	31
4.1.2.1.	Further use for other law enforcement purposes.....	31
4.1.2.2.	Further use for other purposes than law enforcement within the UK.....	32
4.1.2.3.	Further use in the context of onward transfers outside the UK.....	32

4.1.3. Oversight	32
4.2. General legal framework on data protection in the field of national security	33
4.2.1. National security certificates.....	33
4.2.2. Right to rectification and erasure.....	34
4.2.3. Exemptions for National Security	34
4.3. Access and use by UK public authorities for national security purposes.....	34
4.3.1. Legal bases, limitations and safeguards - Investigatory powers exercised in the context of national security.....	35
4.3.1.1. General remarks.....	35
4.3.1.2. Targeted acquisition and retention of communications data	38
4.3.1.3. Equipment interference	39
4.3.1.4. Bulk interception of data from bearers	39
4.3.1.5. Protection and safeguards for secondary data	41
4.3.1.6. Automated processing of communications data.....	42
4.3.1.7. Compliance risks and incompliant practices of competent Intelligence Community authorities.....	42
4.3.2. Further use of the information collected for national security purposes and overseas disclosure	44
4.3.2.1. Further use, overseas disclosure and the applicable legal framework in the UK	44
4.3.2.2. Overseas disclosure and intelligence sharing in the context of international cooperation	45
4.3.3. Oversight	48
4.3.4. Redress	49

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1. EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision (hereinafter “draft decision”) on the adequate protection of personal data by the United Kingdom (hereinafter “UK”) pursuant to the GDPR on 19 February 2021². Following this, the European Commission initiated the procedure for its formal adoption.
2. On the same date, the European Commission asked for the opinion of the European Data Protection Board (hereinafter “EDPB”)³. The EDPB’s assessment of the adequacy of the level of protection afforded in the UK has been made on the basis of the examination of the draft decision itself, as well as on the basis of an analysis of the documentation made available by the European Commission.
3. The EDPB focused on the assessment of both the general GDPR aspects of the draft decision and on the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the UK legal framework are in place and effective.
4. The EDPB has used as main reference for this work its GDPR Adequacy Referential⁴ adopted in February 2018 and the EPDB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures⁵.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² See European Commission’s press release, Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

³ Idem.

⁴ See Article 29 Working Party, Adequacy Referential, adopted on 28 November 2017, as last revised and adopted on 6 February 2018, WP254 rev.01 (endorsed by the EDPB, see <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>); (hereinafter “GDPR Adequacy Referential”).

⁵ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Areas of convergence

5. The EDPB's key objective is to give an opinion to the European Commission on the adequacy of the level of protection afforded to individuals in the UK. It is important to recognise that the EDPB does not expect the UK legal framework to replicate European data protection law.
6. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 45 GDPR and the case-law of the Court of Justice of the European Union (hereinafter "CJEU") require the third country's legislation to be aligned with the essence of the fundamental principles enshrined in the GDPR. The UK data protection framework is largely based on the EU data protection framework (in particular the GDPR and Directive (EU) 2016/680 of the European Parliament and of the Council, hereinafter "EU Law Enforcement Directive" or "LED") which derives from the fact that the UK was a Member State of the EU up until 31 January 2020. Moreover, the UK Data Protection Act 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, further specifies the application of the GDPR in UK law, in addition to transposing the EU Law Enforcement Directive, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK Information Commissioner's Office (hereinafter "ICO"). Therefore the EDPB recognises that the UK has mirrored, for the most part, the GDPR in its data protection framework.
7. **When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent.**
8. In the area of data protection, the EDPB notes that there is a strong alignment between the GDPR framework and the UK legal framework on certain core provisions such as, for example, concepts (e.g., "personal data"; "processing of personal data"; "data controller"); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; direct marketing; automated decision making and profiling.

1.2. Challenges

9. The United Kingdom was until recently a Member State of the EU; therefore, when analysing its law and practice, the EDPB has identified many aspects to be essentially equivalent. At the same time, in view of its role in the process of adopting an adequacy finding but also the time constraints, the EDPB has decided to focus its attention to those aspects where it considers that there is a need for closer look and more detailed scrutiny.
10. Nonetheless, challenges remain and the EDPB considers the following items should be further assessed to ensure that the essentially equivalent level of protection is met, and should be closely monitored in the UK by the European Commission.

1.2.1. General

11. The first challenge, a general one, relates to the monitoring of the evolution of the UK legal system on data protection as a whole. Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection with a possible will to diverge from EU data protection law. Such political declarations have not materialised yet in the UK legal framework. However, this possible future **divergence might create risks for the maintenance of the level of protection provided to personal data transferred from the EU. Therefore, the European Commission is invited to closely monitor such evolutions from the entry into force of its adequacy**

decision and take necessary actions including by amending and/or suspending the decision if necessary.

1.2.2. General data protection aspects

12. First, the so-called ‘immigration exemption’, laid down under **Schedule 2 to the Data Protection Act 2018, Part 1**, paragraph 4, is ‘broadly’ formulated. In particular, it also applies in case personal data are not collected for the purpose of immigration control by a controller, but are made available by the latter to another controller who processes such personal data for the purpose of immigration control.
13. The EDPB invites the European Commission to verify the state of play of the proceedings *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* and, since this judgment is not final (*res judicata*), to verify whether it is confirmed or reviewed by the appeal judgment, taking any update in this regard into account, and specifying it in the decision. **The EDPB calls also on the European Commission to provide in the adequacy decision further information on the immigration exemption⁶, in particular in relation to the necessity and proportionality of such broad exemption in UK law, notably having regard to the broad scope of application *ratione personae*.** At the same time, the EDPB invites the European Commission to further explore whether additional safeguards exist in the UK legal framework or could be envisaged, for instance through legally binding instruments that would complement the immigration exemption by enhancing its foreseeability and the safeguards for the data subjects, also allowing for a better and prompt assessment and monitoring of the necessity and proportionality requirements.
14. Second, although the EDPB recognises that the UK has mirrored, for the most part, Chapter V GDPR in its data protection framework, the EDPB has identified certain aspects of the UK legal framework **with regard to onward transfers** that might undermine the level of protection of personal data transferred from the EEA.
15. Indeed, Article 44 GDPR⁷ provides that transfers and onward transfers of personal data shall only take place if the level of protection of natural persons guaranteed by the GDPR is not undermined. **This means that not only the UK legislation shall be “essentially equivalent” to the EU legislation with regard to the processing of personal data transferred to the UK under the future adequacy decision, but also that the rules applicable in the UK with regard to the onward transfer of those data to third countries shall ensure that an essentially equivalent level of protection will continue to be provided.**

⁶ Also as outcome of the ongoing review of the use of the immigration exemption referred to at p. 5 of the UK Government’s Explanatory Framework for Adequacy Discussions, Section E3: Schedule 2 Restrictions, 13 March 2020,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E - Narrative on Restrictions.pdf.

⁷ “Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the Controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.”

16. Although the EDPB notes the capacity of the UK, under its legal framework, to recognise territories as providing an adequate level of data protection in light of the UK data protection framework, the EDPB wishes to highlight that these territories might not benefit, to date, from an adequacy decision issued by the European Commission and ensure a level of protection “essentially equivalent” to that guaranteed in the EEA. This might lead to possible risks in the protection provided to personal data transferred from the EEA especially if, in the future, the UK data protection framework deviates from the EU acquis. In addition, the UK has already recognised as adequate the third countries that enjoy an adequacy finding by the European Commission under Directive 95/46/EC⁸, while the European Commission will soon review these findings, and the conclusions of this review are not yet known.
17. **For the above situations, the European Commission should fulfil its monitoring role, and in case the essentially equivalent level of protection of personal data transferred from the EEA is not maintained, the European Commission should consider amending the adequacy decision to introduce specific safeguards for data transferred from the EEA and/or to suspend the adequacy decision.**
18. **Regarding international agreements concluded between the UK and third countries,** the European Commission is invited to examine the interplay between the UK data protection framework and its international commitments, beyond the Agreement on access to electronic data for the purpose of countering serious crime concluded between UK and the United States of America (hereinafter “US”)⁹ (hereinafter “UK-US CLOUD Act Agreement”), in particular to ensure the continuity of the level of protection where personal data are transferred from the EU to the UK on the basis of the UK adequacy decision, and then onward transferred to other third countries; and to continuously monitor and take action, where necessary, in the event that the conclusion of international agreements between the UK and third countries risks to undermine the level of protection of personal data provided for in the EU.
19. Furthermore, the European Commission is invited to monitor whether the UK-US CLOUD Act Agreement ensures appropriate additional safeguards, taking into account the level of sensitivity of the categories of data concerned and the sole requirements of the transfer of electronic evidence directly by service providers rather than between authorities, also assessing under which circumstances safeguards may be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement¹⁰.
20. Further, the EDPB notes that onward transfers can also take place from the UK to another third country based on **transfer tools pursuant to the UK applicable data protection legislation**¹¹. Following *Schrems II*¹², the EDPB invites the European Commission to provide reassurances in the

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

⁹ See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019, <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019>.

¹⁰ See Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, December 2016 (hereinafter “EU-US Umbrella Agreement”), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%63A3104_8.

¹¹ See Articles 46 and 47 UK GDPR.

¹² See *Schrems II*.

adequacy decision that necessary safeguards will be effectively put in place taking also into account the legislation of the receiving third country.

21. Concerning the absence **of protections provided under Article 48 GDPR** in the UK legislation, the EDPB invites the European Commission to provide further assurances and specific references to the UK legislation that ensure that the level of protection under the UK legal framework is essentially equivalent to the level of protection guaranteed in the EEA.
22. With regard to **procedural and enforcement mechanisms**, the EDPB notes that the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance; and a system of access to appropriate redress mechanisms equipping individuals in the EEA with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress are key elements a data protection framework consistent with the European one must be characterized by.
23. The EDPB acknowledges that the UK has mirrored in most parts the relevant provisions of the GDPR in the UK GDPR and in the Data Protection Act 2018; nevertheless, the European Commission is invited to continuously monitor any developments in the UK legal framework and practice, which might lead to detrimental impacts on those areas.

[1.2.3. On the access by public authorities to data transferred to the UK](#)

24. The EDPB notes the significant changes in the UK legal framework applicable to security and intelligence agencies, especially regarding the interception and acquisition of communication data. The EDPB understands that these changes are, *inter alia*, a response to the proceedings initiated before the CJEU and the European Court on Human Rights (hereinafter “ECtHR”) and their recent judgments in this context.
25. In particular, the EDPB welcomes the fact that the UK has established the Investigatory Powers Tribunal (hereinafter “IPT”). The IPT is not only competent to hear cases on the use of investigatory powers by law enforcement authorities, but also by intelligence services. It is therefore the understanding of the EDPB that the IPT functions as a proper court in the meaning of Article 47 Charter of Fundamental Rights of the European Union (hereinafter “EU Charter”).
26. Furthermore, the EDPB positively notes the introduction of “Judicial Commissioners” in the Investigatory Powers Act 2016 (hereinafter “IPA 2016”) as a significant improvement. It understands that an important function of the Judicial Commissioners is to approve *ex ante* in individual cases different surveillance measures, including targeted interception and bulk acquisition of communication data (so-called “double lock” procedure).
27. However, in order to assess the effectiveness of this additional level of oversight, the EDPB sees the need to further clarification of the scenarios for which a lawful interception without approval by the Investigatory Powers Commissioner (hereinafter “IPC”) or the Judicial Commissioners is possible, and invites the European Commission to further assess and demonstrate that, even in cases where the double-lock procedure does not apply, the UK legal framework provides for appropriate safeguards, including through effective *ex post* oversight and redress possibilities offered to individuals, thus ensuring a level of protection which is essentially equivalent to the one provided within the EU.
28. Furthermore, the EDPB invites the European Commission to further assess the conditions under which urgency can be invoked, and provide clarifications concerning the possible avenues for the exercise of rights for the data subjects concerned and possible redress avenues offered to them in

the context of equipment interference operations, especially in the case of a derogation to the double-lock procedure.

29. In addition, the EDPB considers that there is a need for further clarification and assessment of bulk interceptions, in particular on the selection and application of the selectors, in order to clarify the extent to which access to personal data meets the threshold set by the CJEU, and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data. An independent assessment from competent UK oversight authorities would be particularly useful. The EDPB also underlines that it seems all the more critical that “overseas-related communications” which are within the scope of bulk interception practices appear to imply that data could be directly intercepted and collected in bulk within the EU by the UK, including for data in transit between the EU and the UK, which would fall within the scope of the draft decision. Given the importance of this aspect, the EDPB calls on the European Commission to closely monitor developments in this regard.
30. Still in relation to bulk interception, the EDPB stresses the consistent assessment by the ECtHR and the CJEU, and recalls the concerns expressed in relation to secondary data, which should benefit from specific safeguards due to their sensitivity. The EDPB therefore calls on the European Commission to carefully assess whether the safeguards provided under UK law for such category of personal data ensure an essentially equivalent level of protection to the one guaranteed in the EEA.
31. In this context, the EDPB is aware of the fact that the 2016 Intelligence and Security Committee’s public report concerning the use of bulk powers¹³ concerns practices under the previous legal framework, which was subsequently replaced by the IPA 2016. Nevertheless, it sees a need for further independent assessment and oversight of the use of automated processing tools by the competent UK oversight authorities, and calls on the European Commission to further assess this issue and the safeguards that would and/or could be afforded to EEA data subjects in this context.
32. The EDPB shares the view expressed by the IPC that further review and monitoring are needed to ensure that the safeguards, applied in practice by competent authorities in the field of national security and intelligence to remedy incompliances with the application of the relevant legislation, are maintained and will continue to be improved. The EDPB also welcomes the fact that consequently, the IPC conducted a review of its approach to inspecting bulk interception in 2019, *“which included a careful review of the technically complex ways in which bulk interception is actually implemented”* and committed to include *“a detailed examination of the selectors and search criteria alluded to above by the ECtHR”* in the inspections of bulk interception from 2020 onwards. Given the importance of this aspect, the EDPB is concerned that detailed examination of the selectors and search criteria has not been carried out yet by the IPC, and calls on the European Commission to closely monitor developments in this regard, especially since the concrete format of such oversight remains to be clarified.
33. The EDPB underlines that, when it comes to overseas disclosures, the application of national security exemption provided under UK law may lead to the absence of safeguards ensuring that the principles of purpose limitation, necessity and proportionality would also be respected or foreseeing that sufficient rights of the individuals, oversight and redress would also be provided or respected in the third country of destination. The EDPB therefore recommends the European Commission to further

¹³ See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>.

examine the overall safeguards provided under UK law when it comes to overseas disclosure, in particular in light of the application of national security exemptions.

34. Finally, the EDPB is concerned about other forms of information sharing and disclosures, on the basis of other instruments, in particular the various international agreements concluded by the UK with other third countries, especially where these instruments remain inaccessible to the public, such as the UK-US Communication Intelligence Agreement. The effect of such agreement could lead to a circumvention of the safeguards identified in relation to the access and use of personal data for national security purposes. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purpose of intelligence cooperation, providing a legal basis for direct interception and acquisition of personal data or the transfer of personal data to these countries may also significantly affect the conditions for further use of the information collected, since such agreements are likely to affect the UK data protection legal framework as assessed.

[1.3. Conclusion](#)

35. The EDPB considers that the UK adequacy assessment is unique because of the previous status of the UK as an EU Member State. Besides, it would also be the first adequacy decision including a sunset clause.
36. Accordingly, the EDPB recognises many areas of convergence between the UK and the EU data protection frameworks. At the same time, however, and following a careful analysis of the European Commission's draft decision and the UK data protection legislation, the EDPB has identified a number of challenges, which are examined extensively in this opinion. In this context, the EDPB wishes to emphasise the paramount role of the European Commission on the monitoring of all relevant developments in the UK.
37. In light of the above, the EDPB recommends the European Commission to address the challenges raised in this opinion. The EDPB also invites the European Commission to monitor closely all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data, and to take swiftly appropriate actions, where necessary.

[2. INTRODUCTION](#)

[2.1. UK data protection framework](#)

38. The UK data protection framework is largely based on the EU data protection framework (in particular the GDPR and the LED), which derives from the fact that the UK was a Member State of the EU up until 31 January 2020. Moreover, the UK Data Protection Act 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, further specifies the application of the GDPR in UK law, in addition to transposing the EU Law Enforcement Directive, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK ICO.
39. As mentioned in recital 12 of the European Commission's draft decision, the UK Government enacted the European Union (Withdrawal) Act 2018, which incorporates directly applicable EU legislation into the law of the UK. Under this Act, the ministers of the UK have the power to introduce secondary legislation, via statutory instruments, to make the necessary modifications to retained EU law following the UK's withdrawal from the EU to fit the domestic context.

40. Consequently, the relevant legal framework applicable in the UK after the end of the transition period¹⁴ consists of:

- the United Kingdom General Data Protection Regulation (hereinafter “UK GDPR”), as incorporated into the law of the UK under the European Union (Withdrawal) Act 2018, as amended by the DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;
- the Data Protection Act 2018 (hereinafter “DPA 2018”), as amended by the DPPEC Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; and
- the IPA 2016.

(together “the UK Data Protection Framework”).

2.2. Scope of the EDPB’s assessment

41. The draft decision of the European Commission is the result of an assessment of the UK Data Protection Framework, followed by discussions with the UK Government. In accordance with Article 70(1)(s) GDPR, the EDPB is expected to provide an independent opinion on the European Commission’s findings, identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these.
42. As mentioned in the GDPR Adequacy Referential: *“the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country”*¹⁵.
43. In this regard, it is to be noted that the EDPB only partially received documents relevant for the examination of the UK legal framework on time. The EDPB received most part of the UK legislation referred to in the draft decision through links referenced in the latter. The European Commission was not in a position to provide the EDPB with written explanations and commitments from the UK in relation to the exchanges between the UK authorities and the European Commission relevant to this exercise¹⁶.

¹⁴ The transition period is set for 31 December 2020, after which date EU law no longer applies in the UK. The “bridge period” is set for 30 June 2021 at the latest, and refers to the additional period during which transmission of personal data from the EEA to the UK is not deemed a transfer.

¹⁵ See WP254 rev.01, p. 3.

¹⁶ With regard to: Article 48 GDPR (footnote 78 of the draft decision); enhanced safeguards and security measures applied by controllers when processing in the national security context (footnote 64 of the draft decision); to the requirement for the controller to consider whether there is a need to rely on the exemption on a case-by-case basis even where a national security certificate has been issued (recital 126 and footnote 172 of the draft decision); the fact that the protections of the EU-US Umbrella Agreement will apply to all personal information produced or preserved under the UK-US CLOUD Act Agreement, irrespective of the nature or type of body making the request, with regard to the details of the concrete implementation of the data protection safeguards which are still subject to discussions between the UK and the US, the confirmation that UK authorities will only let this Agreement enter into force once they are satisfied that its implementation complies with the legal obligations provided therein, including clarity with respect to compliance with the data protection standards for any data requested under this Agreement (recital 153 of the draft decision); situations where data are transferred from the EU to the UK within the scope of this draft decision, and the fact that there would always be a “British Islands connection” and any equipment interference covering such data would

- 44. Taking into account the above, and due to the limited timeframe (2 months) afforded to the EDPB to adopt this opinion, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them.
- 45. When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent. In view of its role in the process of adopting an adequacy finding and the amount of law and practice to be analysed, the EDPB has decided to focus its attention to those aspects where it saw the greatest need to look closer. In addition, in line with the jurisprudence of the CJEU, a very important part of the analysis covers the legal regime of national security access to the personal data transferred to the UK, and the practice of the national security apparatus in the UK. However, it has to be borne in mind that national security is evidently an area of law and practice where the legislation of Member States is not harmonised at EU level and therefore may differ.
- 46. The EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 EU Charter, respectively protecting the right to private and family life, the right to protection of personal data, and the right to an effective remedy and fair trial; and Article 8 of the European Convention on Human Rights (hereinafter “ECHR”), protecting the right to private and family life. In addition to the above, the EDPB considered the requirements of the GDPR, as well as the relevant case-law.
- 47. The objective of this exercise is to provide the European Commission with an opinion on the assessment of the adequacy of the level of protection in the UK. The concept of “adequate level of protection”, which already existed under Directive 95/46/EC, has been further developed by the CJEU. It is important to recall the standard set by the CJEU in *Schrems I*, namely that – while the “level of protection” in the third country must be “essentially equivalent” to that guaranteed in the EU – *“the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU”*¹⁷. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing, and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules¹⁸.

2.3. General comments and concerns

therefore be subject to the mandatory warrant requirement of section 13(1) of the IPA 2016 (recital 206 of the draft decision); and the examples of operational purposes provided (recital 216 and footnote 369 of the draft decision).

¹⁷ See CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650 (hereinafter “*Schrems I*”), paras. 73-74.

¹⁸ See WP254 rev.01, p.2.

2.3.1. International commitments entered into by the UK

48. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential¹⁹, when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter "Convention 108"),²⁰ and its Additional Protocol²¹, should be taken into account.
49. In this regard, the EDPB welcomes that the UK has adhered to the ECHR and is under the jurisdiction of the ECtHR. In addition, the UK has also adhered to Convention 108 and its Additional Protocol, has signed Convention 108+²² in 2018, and is currently working on its ratification.

2.3.2. Possible future divergence of the UK Data Protection Framework

50. As mentioned in recital 281 of the draft decision, the European Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement²³, the UK administers, applies and enforces its own data protection regime, and as soon as the bridge provision under Article FINPROV.10A of the EU-UK Trade and Cooperation Agreement²⁴ ceases to apply, this may notably involve amendments or changes to the data protection framework assessed in the draft decision, as well as other relevant developments.
51. The European Commission has therefore decided to include a sunset clause in its draft decision²⁵, setting the expiration date of four years after its entry into force.
52. It is important to note that the possibility of the UK ministers and the UK Secretary of State to introduce secondary legislation following the end of the bridge period may lead to a significant divergence of the UK Data Protection Framework from the EU's in the future.
53. Indeed, the UK Government has indicated its intention to develop separate and independent policies in data protection, which may then lead to a divergence from EU data protection law²⁶. This intention

¹⁹ See WP254 rev.01, p.2.

²⁰ See Convention for the protection of individuals with regard to the processing of personal data, Convention 108, 28 January 1981.

²¹ See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, opened for signature on 8 November 2001.

²² See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108+"), 18 May 2018.

²³ See Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 029, 31.1.2020, p. 7).

²⁴ See Trade and cooperation agreement between the European union and the European atomic energy community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 444, 31.12.2020, p. 14).

²⁵ See Article 4 of the draft decision. See also recital 282 of the draft decision.

²⁶ The UK's National Data Strategy (last updated on 9 December 2020, <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy>) includes the following as one of its missions: "*Championing the international flow of data. The flow of information across borders fuels global business operations, supply chains and trade, powering growth across the world. It also plays a wider societal role. The transfer of personal data ensures people's salaries are paid, and helps them connect with loved ones from afar. And, as the coronavirus pandemic has demonstrated, sharing health data*

encompasses the inclusion of personal data aspects in trade agreements²⁷, a practice that entails the risk of lowering the level of protection of personal data provided for by the UK²⁸.

54. Finally, not only since the end of the transition period, the UK is no longer bound by CJEU case-law but also, the already adopted judgments of the CJEU, considered as retained case law in the UK legal framework, might not bind the UK any more as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period and its Supreme Court is not bound by any retained EU case-law²⁹.
55. **Considering the risks related to the possible deviation of the UK Data Protection Framework from the EU acquis following the end of the bridge period, the EDPB welcomes the European Commission’s decision to introduce a sunset clause of four years for the draft decision. However, the EDPB would like to highlight here the importance of the European Commission’s monitoring role³⁰. Indeed, the European Commission should monitor all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data transferred under the UK adequacy decision on an ongoing and permanent basis from its entry into force. In addition, the European Commission should take appropriate action by suspending, amending or repealing the adequacy decision, based on the circumstances at hand, if after the adequacy decision is adopted, the European Commission has indications that an adequate level of protection is no longer ensured in the UK.**
56. On its side, the EDPB will use its best efforts to inform the European Commission about any relevant action undertaken by Member State’s data protection supervisory authorities (hereinafter “SAs”) either in the commercial or public sector, and in particular regarding complaints made by data subjects in the EEA concerning the transfer of personal data from the EEA to the UK.

can aid vital scientific research into diseases while uniting countries in their response to global health emergencies. Having left the European Union, the UK will champion the benefits that data can deliver. We will promote domestic best practice and work with international partners to ensure data is not inappropriately constrained by national borders and fragmented regulatory regimes so that it can be used to its full potential.” (emphasis added).

²⁷ Ibid: “Facilitate cross-border data flows: **We will work globally to remove unnecessary barriers to international data flows. We will agree ambitious data provisions in our trade negotiations** and use our newly independent seat in the World Trade Organisation to influence trade rules for data for the better. **We will remove obstacles to international data transfers** which support growth and innovation, including by developing a new UK capability that delivers new and innovative mechanisms for international data transfers. We will also work with partners in the G20 to create interoperability between national data regimes to minimise friction when transferring data between different countries”. (emphasis added).

²⁸ See European Parliament resolution of 12 December 2017 “Towards a digital trade strategy” (2017/2065(INI)), Section V, in which it stressed that “The protection of personal data is non-negotiable in [EU] trade agreements”, available at: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_EN.pdf. See also, European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, para. 28 in which it is stated: “supports the Commission’s practice of addressing data protection and personal data flows separately from trade agreements”, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_EN.html.

²⁹ See section 6(3) to (6) EU (Withdrawal) Act 2018.

³⁰ See Article 45(4) GDPR.

3. GENERAL DATA PROTECTION ASPECTS

3.1. Content principles

57. Chapter 3 of the GDPR Adequacy Referential is dedicated to the “Content Principles”. A third country’s system must contain them in order for its level of data protection to be considered essentially equivalent to the one guaranteed within the EU. The EDPB acknowledges the fact that the UK does not have a codified constitution in that there is no one single document that sets out its governing fundamental rules. However, the right to respect for private and family life (and the right to data protection as part of that right) and the right to a fair trial³¹ are included in the Human Rights Act 1998, and the constitutional value of this statute has been recognised by UK courts. Indeed, the Human Rights Act 1998 incorporates the rights contained in the ECHR³². In addition, the Human Rights Act 1998 states very importantly that any action of public authorities must be compatible with the ECHR³³.
58. Aside from structural and formalistic differences between the UK and EU legislation, the EDPB notes, as one can expect, that the UK’s approach to data protection is similar to the one in the EU resulting from the fact that the UK was a Member State of the EU up until 31 January 2020. As a result, many content principles are aligned with the GDPR’s; therefore provide a level of protection essentially equivalent to the one provided by the EU. The EDPB has decided not to develop further the analysis as to those content principles that are in alignment with EU legislation, and is satisfied with the analysis provided by the European Commission in its draft decision. Such content principles are for example the following: concepts (e.g., “personal data”; “processing of personal data”; “data controller”); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; special categories of data; direct marketing; automated decision making and profiling. The EDPB further notes that the UK GDPR and the DPA 2018 include content principles that go further than what is required by the GDPR Adequacy Referential and mirror the principles included in the GDPR; therefore elevating the level of protection provided for in the UK. Such content principles are for example the ones related to personal data breach notifications, the data protection officer, data protection impact assessments and data protection by design and by default.
59. However, as mentioned in the Introduction, the EDPB wishes to specifically address in this opinion certain points on which the EDPB has concerns and would like to request clarifications from the European Commission.

3.1.1. Rights of access, rectification, erasure and objection

60. The so-called ‘immigration exemption’, laid down under **Schedule 2 to the DPA 2018, Part 1**, paragraph 4 allows controllers involved in “immigration control” to not apply certain data subjects’ rights provided by the DPA 2018 if this would be likely to “*prejudice the maintenance of effective immigration control*” or “*the investigation or detection of activities that would undermine the maintenance of effective immigration control*”.

³¹ See Articles 6 and 8 ECHR (Schedule 1 to the Human Rights Act 1998).

³² For more information, see recitals 8-10 of the draft decision.

³³ See section 6 Human Rights Act 1998.

61. As acknowledged by the European Commission in its draft decision³⁴, and referred to in the Opinion of the LIBE Committee of the European Parliament, on the conclusion, on behalf of the EU, of the Trade and Cooperation Agreement between the EU and the UK³⁵, this exemption is '**broadly formulated**'. It applies to the following rights: right to be informed; right of access; right to erasure; right to restrict processing; and right to object.
62. Besides, it is important to note that this exemption also applies in case personal data are not collected for the purpose of immigration control by a controller ("controller 1"), but are however made available by the latter to another controller ("controller 2") who processes such personal data for the purpose of immigration control (e.g., the UK Home Office)³⁶.
63. In *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (03 October 2019)*, the applicants challenged the lawfulness of the immigration exemption on the ground that it was contrary to Article 23 GDPR and incompatible with the rights guaranteed by Articles 7 and 8 EU Charter relating to privacy and the protection of personal data. The High Court of England and Wales (hereinafter "High Court") considered whether the immigration exemption in paragraph 4 of Part 1 of Schedule 2 of the DPA 2018 is lawful, and concluded in favour of its lawfulness.
64. The High Court considered in particular that:

³⁴ See recitals 62-65 of the draft decision.

³⁵ In this regard, on the **broad formulation** of the immigration exemption, see Opinion of the Committee on Civil Liberties, Justice and Home Affairs on the conclusion, on behalf of the Union, of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part and the United Kingdom of Great Britain and Northern Ireland, of the other part, and of the Agreement between the European Union and United Kingdom of Great Britain and Northern Ireland concerning security procedures for exchanging and protecting classified information (2020/0382(NLE)), 5 February 2021, https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_EN.pdf, para. 10: "recalls, in this regard, Parliament's February and June 2020 resolutions, pointing out the **general and broad exemption** for the processing of personal data for immigration purposes of the UK Data Protection Act", and para. 11: "considers that the **general and broad** exemption for the processing of personal data for immigration purposes of the UK Data Protection Act [...] need to be amended before a valid adequacy decision can be granted;"(emphasis added).

³⁶ See example provided in the ICO "Guide to the General Data Protection Regulation (GDPR)", v 01 January 2021, p. 307 (emphasis added): "A private organisation (controller 1) alerts the Home Office (controller 2) to an employee who is believed to have submitted false documents to evidence their identity and qualifications to obtain a job. The employer provides the Home Office with the relevant information. The right of the individual to be informed that their personal data has been passed to the Home Office is restricted in so far as giving effect to it would be likely to prejudice the investigation.

The employer is therefore under no obligation to inform the individual that their information has been passed to the Home Office, and in turn the Home Office is under no obligation to provide the individual with a privacy notice informing them that it is now processing their personal data. The exemption applies to both controllers to the same extent.

However, the employee requests a copy of their personal data from the Home Office which is now investigating them. The Home Office may rely on the exemption to withhold part of their data if the disclosure would be likely to prejudice the investigation. Should the employee make a similar request to their employer, they would also be able to apply the exemption to the same extent."

In other words, as clarified on p. 300: "*In the majority of cases the Home Office, or one of its agencies and contractors, will be the controller applying this exemption. However, it is important to note that the application of this exemption is not just limited to the Home Office. It may also be relevant to other controllers such as employers, universities and the police, who liaise with the Home Office on immigration matters."*

- “[...] the Immigration Exemption is plainly a matter of “important public interest” and pursues a legitimate aim.[...], para. 30;
 - “the Immigration Exemption satisfies the requirements for a measure to be “in accordance with the law. [...]”, para. 38;
 - “The Immigration Exemption may only be relied on if and to the extent that compliance with “the listed GDPR provisions” **would be likely to prejudice** the maintenance of effective immigration control or the investigation or detection of activities that would undermine the maintenance of effective immigration control. The words “would be likely to prejudice”, in the context of the Data Protection Act 1998 (which preceded the DPA 2018), were interpreted to mean “a very significant and weighty chance of prejudice to the particular public interest. The degree of risk must be such that there ‘may very well’ be prejudice to those interests, even if the risk falls far short of being more probable than not [...].”, para. 39 (emphasis added).
65. It should be noted that this judgment is, to the EDPB’s knowledge, not final and has been appealed.
66. As specified in the EDPB Guidelines on restrictions under Article 23 GDPR (“the Article 23 GDPR Guidelines”)³⁷ “[...] in a GDPR context, restrictions shall be **provided for in a legislative measure, concern a limited number of rights of data subjects and/or controller’s obligations** which are listed in Article 23 of the GDPR, **respect the essence** of the fundamental rights and freedoms at issue, be a **necessary and proportionate measure** in a democratic society and safeguard one of the grounds set out in Article 23(1) of the GDPR [...].”³⁸
67. The EDPB also recalls that recital 41 GDPR states that “[w]here this Regulation refers to **a legal basis or a legislative measure**, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be **clear and precise and its application should be foreseeable to persons subject to it**, in accordance with the case-law of the Court of Justice of the European Union [...] and the European Court of Human Rights” (emphasis added).
68. Although the ECtHR specified that “[f]urther, as regards the words “in accordance with the law” and “prescribed by law” which appear in Articles 8 to 11 of the Convention, the [ECHR] observes that it has always understood the term “law” in its “substantive” sense, not its “formal” one; it has included both “written law”, encompassing enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament, and unwritten law. “Law” must be understood to include both statutory law and judge-made “law””³⁹, the Article 23 GDPR Guidelines recall that “[a]ccording to the CJEU case law, any **legislative measure** adopted on the basis of Article 23(1) [of the] GDPR must, in particular, **comply with the specific requirements set out in Article 23(2) of the GDPR**. Article 23(2) [of the] GDPR states that the legislative measures imposing restrictions to the rights of data subjects and the controllers’ obligations shall contain, where relevant, **specific provisions about several criteria**

³⁷ See EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR, version 1.0, adopted on 15 December 2020, which are currently under finalisation following public consultation, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en.

³⁸ See Article 23 GDPR Guidelines, para. 9, p. 5.

³⁹ See ECtHR, *Sanoma Uitgevers B.V. v. The Netherlands*, 14 September 2010, EC:ECHR:2010:0914JUD003822403, para. 83 (emphasis added).

outlined below. As a rule, all the requirements detailed below **should be included in the legislative measure** imposing restrictions under Article 23 [of the] GDPR.”⁴⁰

69. It can be observed in this regard that the immigration exemption itself does not specify the following elements referred to under Article 23(2) GDPR:
- “the safeguards to prevent abuse or the unlawful access or transfer” (d);
 - “the controller or categories of controllers” (e)⁴¹;
 - “the risks to the rights and freedoms of data subjects” (g);
 - “the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction” (h).
70. The ICO’s “Guide to the General Data Protection Regulation (GDPR)”⁴², including a Chapter on the “immigration exemption”, does provide clarifications on the immigration exemption, but cannot per se provide binding rules complementing it. Moreover, the issue of ‘quality of the law’ is particularly relevant given the importance of the restricted rights and the extension of the exemption⁴³.

⁴⁰ See Article 23 GDPR Guidelines, paras. 45 and 46, p. 11. Under Article 52(3) EU Charter, “[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection”. On the notion of ‘provided for by law’ under Article 52(1) EU Charter, the criteria developed by the ECtHR should be used as suggested in several CJEU Advocate General’s Opinions, see for example the Opinions in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, paras. 137-154, and in case C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, paras. 88-114. Hence, reference can be made, among others, to the ECtHR ruling in *Weber and Saravia v Germany*, para. 84: “The Court reiterates that the expression “in accordance with the law” within the meaning of Article 8 § 2 [of the ECHR] requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law.” (emphasis added).

See also recital 41 GDPR: “Such [a legal basis or] legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (...) and the European Court of Human Rights” (emphasis supplied).

⁴¹ See the aforementioned High Court case, para. 54: “In my view there is nothing unlawful about the Immigration Exemption being available to all data controllers processing data for the specified purposes. As the defendants point out, without paras 4(3)–(4) the Immigration Exemption would be rendered ineffective in cases where data is obtained from third parties (such as a local authority or HM Revenue and Customs) for the purposes of maintaining effective immigration control.” (emphasis added), hence confirming the generalised application of the restrictions.

⁴² ICO’s “Guide to the General Data Protection Regulation (GDPR)”, v 01 January 2021, p. 299-307.

⁴³ See para. 57 of the aforesaid High Court case: “Mr Knight informs me that the Commissioner is finalising guidance on the Exemption, but it will have “statutory” status only in the sense of being issued by virtue of the Commissioner’s powers under art.57(1) of the GDPR. It will have no legal status under DPA 2018.”

The rationale for the introduction of legally binding guidance supported by ICO is referred to in particular at paras. 56-60 of the judgment:

“56. Finally, I turn to the Commissioner’s submission that without accompanying statutory guidance to provide safeguards as to the meaning and application of the Immigration Exemption, the exemption would not be a proportionate implementation of art.23(1) of the GDPR. Mr Knight says that supplemented by such guidance, the provision is proportionate.

57. Mr Knight informs me that the Commissioner is finalising guidance on the Exemption, but it will have “statutory” status only in the sense of being issued by virtue of the Commissioner’s powers under art.57(1) of

71. *A fortiori*, the “**prejudice test**” does not set out the safeguards to prevent abuse or unlawful access or transfer, and to be implemented for instance by the Home Office.
72. In the light of all of the above, the EDPB remarks that further clarifications on the application of the immigration exemption are needed.
73. Furthermore, the EDPB remarks the lack of a legally binding instrument that clarifies the immigration exemption in view of considering whether it is essentially equivalent with Article 23 GDPR and Articles 7 and 8 EU Charter. At the same time, the EDPB considers that the necessity and proportionality of the broad scope *ratione personae* of the immigration exemption needs to be further demonstrated by the European Commission, supported by evidence.
74. **As a conclusion, the EDPB invites the European Commission to verify the state of play of the proceedings *Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)* referred to above and, since this judgment is not final (*res judicata*), to verify whether it is confirmed or reviewed by the appeal judgment, to take any update in this regard into account, and to specify it in the adequacy decision. The EDPB also calls on the European Commission to provide further information on the necessity and**

the GDPR. It will have no legal status under [DPA 2018](#). I understand also that the Home Office has produced draft internal staff guidance on the Immigration Exemption (see [22] above). In practice guidance issued by the Commissioner is influential regardless of its legal basis. However, there is no power for the Commissioner to issue “binding” guidance of the sort that the Supreme Court had in mind in the [Christian Institute](#) case (at [101] and [107]). It appears that primary legislation would be required if it were considered necessary for there to be guidance on the Immigration Exemption of the same status as the codes of practice currently provided for in [ss.121–124 of DPA 2018](#).

58. In his argument for statutory guidance Mr Knight contends that the context in which the use of the Immigration Exemption will arise necessarily frames the concerns about the necessity and proportionality of its existence and use. He draws attention to two matters in particular in the legal context. First, personal data to which the Immigration Exemption is applied is inherently likely to involve special category data within the meaning of art.9(1) of the GDPR (i.e. data “revealing racial or ethnic origin”). Such data is identified in the GDPR because it requires a higher measure of protection ([Opinion 1/15 \[2019\] 3 C.M.L.R. 25](#) at [141]). Secondly, it is a basic proposition of data protection law that the right of subject access in particular is of great importance as the gateway to being able to exercise the other rights provided to data subjects (see [YS v Minister voor Immigratie, Integratie en Asiel \(C-141/12\) EU:C:2014:2081; \[2015\] 1 C.M.L.R. 18](#) at [44]).

59. Mr Knight identifies four points of a practical nature. First, when controllers do not explain to data subjects that they have relied upon a statutory exemption, nor provide a broad summary of the reasons why, the data subject will be unaware that the exemption has been applied, and unable to challenge it effectively as a result. Secondly, data subjects will be especially reliant on controllers to apply the exemption with care and only so far as necessary. Although any data subject is entitled to complain to the Commissioner about the application of the exemption, or to bring legal proceedings before the courts, it is likely that the data subject will be unaware of their rights and lack the funds to take legal steps, in circumstances where there is a need for prompt and accurate compliance with data protection rights. Thirdly, as an immigrant the data subject is likely to be in a vulnerable position. Fourthly, this is not an abstract issue in the light of the defendants’ evidence as to the use of the Immigration Exemption (see [4] above).

60. Mr Knight suggests that there is a close parallel between the present challenge to the Immigration Exemption and the reasoning of the Court in [Christian Institute \[2016\] UKSC 51](#) . As in [Christian Institute](#) , he contends, the Immigration Exemption is wide, uses undefined terms, applies a low threshold, is subject to controls not apparent on the face of the provision and applies to a very broad array of contexts and rights. Unlike [Christian Institute](#) there is no publicly available guidance, still less of a statutory status even to which regard must be had, on the Immigration Exemption.”

proportionality of the immigration exemption, in particular having regard to the broad scope of application *ratione personae*.

75. At the same time, the EDPB invites the European Commission to further explore whether additional safeguards exist in the UK legal framework or could be envisaged, for instance through legally binding instruments that would complement the immigration exemption enhancing its foreseeability by and the safeguards for data subjects, also allowing for a better and prompt assessment and monitoring of the necessity and proportionality requirements.

3.1.2. Restrictions on onward transfers

76. Article 44 GDPR provides that transfers and onward transfers of personal data shall only take place if the level of protection of natural persons guaranteed by the GDPR is not undermined. Therefore, personal data transferred from the EEA to the UK based on the adequacy decision shall enjoy an essentially equivalent level of protection to the one provided under the EU data protection framework. This means that not only the UK legislation shall be “essentially equivalent” to the EU legislation with regard to the processing of personal data transferred to the UK under the draft decision, but also that the rules applicable in the UK with regard to the onward transfer of those data to third countries shall ensure that an essentially equivalent level of protection will continue to be provided.
77. As a result, it is important that any onward transfer from the UK to another third country of personal data from the EEA is properly protected with safeguards, or is carried out in accordance with the rules on derogations⁴⁴ to ensure the continuity of protection afforded by the EU legislation. Indeed, if no such protection can be provided, onward transfers of EEA personal data should not take place.
78. The EDPB recognises that the UK has mirrored, for the most part, Chapter V GDPR in the UK GDPR (Articles 44-49) and in the DPA 2018⁴⁵. However, the EDPB has identified certain aspects of the UK legislative framework with regard to onward transfers that might undermine the level of protection of personal data transferred from the EEA.
79. The first challenge the EDPB has identified relates to the recognition by the UK, following the procedure as elaborated in the DPA 2018, of third countries, international organisations or territories⁴⁶ as adequate recipients. Indeed, onward transfers of EEA personal data may occur from the UK to other third countries, on the basis of a future possible UK adequacy regulation⁴⁷.
80. More specifically, as explained in recital 77 of the draft decision, the UK Secretary of State has the power to recognise a third country (or a territory or a sector within a third country), an international organisation, or a description of such a country, territory, sector, or organisation as ensuring an adequate level of protection of personal data, following consultation of the ICO⁴⁸. When assessing the adequacy of the level of protection, the UK Secretary of State must consider the same elements that the European Commission is required to assess under Article 45(2)(a)-(c) GDPR, interpreted together with recital 104 GDPR and the retained EU case-law. This means that, when assessing the

⁴⁴ See Article 49 UK GDPR.

⁴⁵ See section 17A, 17B, 17C and 18 DPA 2018.

⁴⁶ See section 17A of DPA 2018 DPA 2018.

⁴⁷ The UK equivalent to an adequacy decision under the GDPR.

⁴⁸ See section 182(2) DPA 2018. See also the Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/>.

adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection “essentially equivalent” to that guaranteed within the UK. Although the EDPB notes the capacity of the UK, under the UK GDPR, to recognise territories as providing an adequate level of protection in light of the UK Data Protection Framework, the EDPB wishes to highlight that these latter territories might not benefit, to date, from an adequacy decision issued by the European Commission recognising a level of protection “essentially equivalent” to that guaranteed in the EU. This might lead to possible risks in the protection provided to personal data transferred from the EEA, especially if the UK Data Protection Framework were to deviate from the EU acquis in the future. It is to be noted that in July 2020, the *Schrems II* CJEU landmark case⁴⁹ resulted in the invalidation of the US Privacy Shield Decision as, according to the CJEU, the US legal framework could not be considered as providing an essentially equivalent level of protection compared to the one of the EU. However, the already adopted judgments of the CJEU, considered as retained case-law in the UK legal framework, might not bind the UK anymore as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period, and its Supreme Court is not bound by any retained EU case law⁵⁰.

81. **The EDPB invites the European Commission to closely monitor the adequacy assessment process and criteria by UK authorities with regard to other third countries, in particular with respect to third countries not recognised as adequate under the GDPR by the EU. Where the European Commission finds that no essentially equivalent level of protection to that guaranteed within the EU is ensured by a third country found adequate by the UK, the EDPB invites the European Commission to take any and all necessary steps such as, for example, amending the UK adequacy decision to introduce specific safeguards for personal data originating from the EEA, and/or to consider the suspension of the UK adequacy decision, where personal data transferred from the EEA to the UK are subject to onward transfers to the third country in question on the basis of a UK adequacy regulation.**
82. **The second challenge** relates to the upcoming review of the already existing adequacy decisions rendered by the European Commission under Directive 95/46/EC. Following this review, the European Commission might decide that certain countries that benefited until now from an adequacy decision no longer provide for an essentially equivalent level of protection taking into account the current EU legislation and recent case-law. However, as provided for in paragraph 4, Schedule 21 DPA 2018, the UK has already recognised those countries as providing for an adequate level of protection. Even though the UK Secretary of State must conduct a review of these adequacy findings within a period of four years, the European Commission notes in its draft decision that these adequacy findings will not automatically cease to exist should the UK Secretary of State not undertake the required review within the stipulated four-year time limit⁵¹.
83. **The EDPB invites the European Commission to monitor whether, once the EU review of the already existing adequacy decisions is finalised, a country, deemed to no longer provide for an adequate level of protection, is still considered as such by the UK. If this is the case, the EDPB invites the European Commission, based on recitals 277 – 280 of the draft decision to take any appropriate measures to remedy the situation, for example by amending the adequacy decision in order to add specific requirements for personal data originating from the EEA and/or by suspending the adequacy decision, if personal data transferred from the EEA to the UK are subject to onward**

⁴⁹ See *Schrems II*.

⁵⁰ See section 6(3) to (6) EU (Withdrawal) Act 2018.

⁵¹ See recital 82 of the draft decision.

transfers to the third country in question. The EDPB invites the European Commission to continue this monitoring exercise for the duration of the UK adequacy decision.

84. **The third challenge** concerns the onward transfer of personal data from the EEA to non-adequate countries based on the transfer tools provided for in Articles 46 and 47 UK GDPR. Although the UK GDPR provides for the same transfer tools as the ones provided by the GDPR, the EDPB highlights the need to ensure that the safeguards they contain provide for an effective protection in the third country, especially in the light of the *Schrems II* judgment.
85. Following the *Schrems II* ruling, in which the CJEU reminds that the protection granted to personal data in the EU must travel with the data wherever it goes, the EDPB has already adopted initial recommendations on supplementary measures⁵² to assist exporters, where required, in ensuring that data subjects are afforded a level of protection essentially equivalent to that guaranteed within the EU.
86. According to the CJEU, data exporters are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the data importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools⁵³. Where this is the case, data exporters should implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law.
87. **The EDPB invites the European Commission, in order to ensure continuity of protection, to introduce in the draft decision reassurances that when the transfer tools provided in Articles 46 and 47 UK GDPR are used by data exporters in the UK for onward transfers to other third countries of EEA transferred data, these data exporters assess on a case-by-case basis, the data protection framework of the third country; and if necessary, take appropriate measures to ensure the effective respect of the safeguards contained in the chosen transfer tool to ensure an essentially equivalent level of protection to that guaranteed within the EU. Without these reassurances, the EDPB stresses that that there is a risk that the essentially equivalent level of protection to the one guaranteed within the EU, will be watered down through onward transfers taking place from the UK.**
88. **The fourth challenge** relating to onward transfers concerns the international agreements concluded, or to be concluded in the future by the UK and the possible direct access, by authorities from third country(ies) party(ies) to such agreements, to personal data from the EEA. Indeed, the EDPB has strong concerns in relation to the already concluded UK-US CLOUD Act Agreement and the European Commission acknowledges this challenge, stressing that "*a possible entry into force of the Agreement may impact the level of protection assessed in this Decision*"⁵⁴. Indeed, based on this agreement, once it enters into force, personal data transferred from the EEA to the UK under the draft decision would then be subject to the provisions of this agreement laying down conditions for direct access by US authorities, impacting the UK Data Protection Framework, including the provisions on onward transfers. As a result, the level of protection provided to the data transferred from the EEA may be

⁵² See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, which are currently under finalisation following public consultation, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransfertools_en.pdf.

⁵³ See *Schrems II*, para. 134.

⁵⁴ See recital 153 of the draft decision.

substantially affected by the provisions of the agreement concluded with the US, and impact on the level of protection for such data. The EDPB notes in this context that the European Commission refers to explanations given by UK authorities in recital 153 of its draft decision, without quoting or providing any concrete written assurance or commitment, nor pointing out specific legal provisions under UK law that would give effect to such explanations.

89. The EDPB has previously raised these concerns in a letter addressed to the European Parliament dated 15 June 2020⁵⁵. The EDPB had highlighted that based on the “*EU acquis in the field of data protection, and in particular with the GDPR and the law enforcement directive*” the EDPB has reservations as to whether the safeguards in the agreement for access to personal data in the UK would apply in certain circumstances requiring disclosure obligations to the US, as well as whether these safeguards are sufficient in light of the EU standards so as to not undermine the level of protection provided in the EU.
90. Furthermore, the provisions of the UK-US CLOUD Act Agreement may significantly affect the substantive and procedural conditions under which personal data held by controllers or processors in the UK can be directly accessed by US authorities, thus impacting on the level of protection guaranteed under UK law. To provide for a level of protection essentially equivalent to the one guaranteed under EU law, it is for example “*essential that the safeguards as per such agreement include a mandatory prior judicial authorisation, as an essential guarantee for access to metadata and content data. On the basis of its preliminary assessment, the EDPB, while noting that the agreement refers to the application of domestic law, could not identify such a clear provision in the agreement concluded between the UK and the US*⁵⁶.”
91. While the European Commission highlights that data obtained under this agreement would benefit from equivalent protections to the specific safeguards provided by the so-called “EU-US Umbrella Agreement”, the EDPB has concerns as to whether the incorporation of these safeguards into the UK-US CLOUD Act Agreement by a mere reference applying on a *mutatis mutandis* basis would meet the criteria of clear, precise and accessible rules when it comes to access to personal data, or would sufficiently enshrine such safeguards to be effective and actionable under UK law.
92. **The EDPB therefore recommends that the European Commission clarifies how and based on which legal instrument equivalent protections to the specific safeguards provided by the EU-US Umbrella Agreement would be given effect and have binding character under UK law.**
93. The EDPB also notes that the provisions of the UK-US CLOUD Act Agreement, read in conjunction with section 3 US CLOUD Act⁵⁷, raises questions as to the actual application of the safeguards offered by the agreement for the access, by US law enforcement authorities, to personal data in the UK processed by providers of electronic communication service or remote computing service (hereinafter “CSPs”) falling under the jurisdiction of the US. Indeed, should a CSP located in the UK be subject to US law (e.g., because it is the subsidiary of a US company), it remains to be ascertained whether US authorities would be bound to rely on the UK-US CLOUD Act Agreement to obtain that data. As the European Commission points out that “[p]articular attention will be given to the application and adaptation of the Umbrella Agreement’s protections to the specific type of transfers covered by the UK-US Agreement”, the EDPB stresses that on the basis of its preliminary assessment,

⁵⁵ See EDPB response to MEPs Sophie in't Veld and Moritz Körner on the US-UK agreement under the US Cloud Act, adopted on 15 June 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

⁵⁶ See the abovementioned EDPB letter.

⁵⁷ See US CLOUD Act, <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>.

it is unclear whether the safeguards enshrined in the UK-US CLOUD Act Agreement, and therefore the one provided by the EU-US Umbrella Agreement, would apply to all, if any, requests for access to data in the UK made by US authorities under the US CLOUD Act.

94. There may be other future international agreements or commitments with third countries the UK might be entering into in the future, and that would apply to personal data transferred from the EEA to the UK under the draft decision⁵⁸. Depending on the provisions of these agreements and the application of specific safeguard clauses, these international agreements, by affecting the UK Data Protection Framework may also significantly impact on the substantive and procedural conditions for access to personal data in the UK by third country authorities. This is in particular the case for the draft second additional protocol to the Council of Europe Convention on Cybercrime (hereinafter “Budapest Convention”) currently being negotiated among the parties to this Convention, which include several non-EU countries. Indeed, the draft protocol includes clauses which can be discretionally activated by the parties, for instance concerning the authorisation to grant access to content data or not. While all EU Member States would activate the clauses in compliance with EU data protection rules, no guarantee has been provided concerning the UK, which could substantially deviate from the level of protection that would then be offered within the EU. Another example of the issues presented above, is the Agreement between the UK and Japan for a Comprehensive Economic Partnership⁵⁹ (“CEPA”), the UK’s first post-Brexit trade deal that entered into force on 1 January 2021⁶⁰ and that includes provisions on personal data⁶¹. The EDPB furthermore notes that the UK has also formally announced on 1 February 2021 its request to join the Comprehensive and Progressive Trans-Pacific Partnership (“CPTPP”) which incorporates the Trans-Pacific Partnership Agreement (“TPP”)⁶².
95. The EDPB notes that, apart from the UK-US CLOUD Act Agreement, the international agreements mentioned above are not addressed in the draft decision.
96. **The EDPB invites the European Commission to:**
- Examine the interplay between the UK Data Protection Framework and its international commitments, beyond the UK-US CLOUD Act Agreement, in particular to ensure the continuity of the level of protection in case of onward transfers to other third countries of personal data transferred from the EEA to the UK on the basis of a UK adequacy decision; and to continuously monitor and take action, where needed, with regard to the conclusion of other international agreements between the UK and third countries that risk to undermine the level of protection of personal data provided for in the EU.

⁵⁸ See section 2.3.3 above.

⁵⁹ See UK/Japan: Agreement for a Comprehensive Economic Partnership [CS Japan No.1/2020], <https://www.gov.uk/government/publications/uk-japan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020>.

⁶⁰ See UK Government’s guidance on UK trade agreements with non-EU countries, <https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries>.

⁶¹ Pursuant to Article 8.80 para. 5 CEPA, the parties commit to encourage the development of mechanisms to promote compatibility between their different legal approaches to (personal) data protection. Pursuant to Article 8.84, the parties commit not to prohibit or restrict the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person within the meaning of CEPA.

⁶² Pursuant to Article 14.11 para. 2 TPP, each party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.

- Provide the EDPB with written commitments from UK authorities and identify specific provisions under UK law, in relation to the explanation related to the possible application and implementation of the UK-US CLOUD Act Agreement as referred to in recital 153 of the draft decision.
 - Monitor, in this context, whether, in addition to the safeguards that could be provided by an appropriate implementation of the adaptation of the EU-US Umbrella Agreement, the UK -US CLOUD Act Agreement ensures appropriate additional safeguards to take into account the level of sensitivity of the categories of data concerned and the unique requirements of the transfer of electronic evidence directly by CSPs rather than between authorities.
 - Assess the impact and potential risks of the provisions on personal data contained in international agreements recently signed by the UK, such as the CEPA.
97. **The fifth challenge** identified relates to the application of derogations for the transfers of personal data to a third country. Although the available derogations under the UK GDPR are the same as the ones provided under the GDPR, it is important that the ICO applies and will continue to apply an interpretation in relation to the use of these derogations aligned with the one of the EDPB. If this is not the case, or if the UK diverges from this interpretation in the future, there would be a risk that the level of protection of data transferred from the EEA to third countries via the UK could be undermined.
98. **The EDPB invites the European Commission, as part of its monitoring task, to specifically check that the UK interpretation on the use of derogations remains aligned to the EU's interpretation.** If however, a different interpretation of the use of derogations were followed by the UK undermining the level of protection, it is essential that the European Commission takes necessary steps by amending the adequacy decision to make sure that the level of protection provided to EEA personal data transferred to the UK will not then be undermined when these data are onward transferred from the UK to third countries on the basis of a different interpretation of derogations.
99. **The sixth challenge**, final one for this section, refers to the absence of protections provided under Article 48 GDPR in the UK Data Protection Framework.
100. The European Commission indeed clarifies in its draft decision that in the absence of adequacy regulations or appropriate safeguards, a transfer can only take place based on derogations set out in Article 49 UK GDPR, "*with the exception of Article 48 of Regulation (EU) 2016/679 that the United Kingdom has chosen not to include in the UK GDPR.*"⁶³ The absence of an essentially equivalent provision to Article 48 GDPR enshrined in the UK Data Protection Framework, in relation to transfers or disclosures, following a judgment of a court or tribunal or a decision of an administrative authority from another third country, may give rise to legal uncertainty as to whether the level of protection for personal data transferred from the EEA to the UK under the draft decision would be substantially affected.
101. In its GDPR Adequacy Referential, the EDPB points out that, when it comes to onward transfers, "*further transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient is also subject to rules affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller.*

⁶³ See footnote 78 of the draft decision.

*controller*⁶⁴. Furthermore, the EDPB stresses that “*the initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing*”⁶⁵. As part of Chapter V GDPR, Article 48 has to be taken fully into account in assessing whether the UK legal framework ensures an essentially equivalent level of protection in this regard⁶⁶.

102. The EDPB emphasises in this context the CJEU case-law in relation to the risk of abuse or unlawful access and use of data, stating in particular that “*as regards the level of protection of fundamental rights and freedoms that is guaranteed within the European Union, EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must, according to the Court’s settled case-law, lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data*”⁶⁷.
103. The EDPB notes in this regard that, based on the information available in the draft decision, the UK Data Protection Framework does not clearly provide that any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement in force between the requesting third country and the UK. Article 48 GDPR is an essential provision under Chapter V GDPR as it requires that a transfer or disclosure of personal data following a judgment or decision from a third country court/tribunal or administrative authority may only be recognised or enforceable if based on an international agreement in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfers pursuant to Chapter V GDPR. Indeed, the EDPB recalls that “*a request from a foreign authority does not in itself constitute a legal ground for transfer. The order can only be recognised if based on an international agreement such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State*”⁶⁸. It is therefore key that essentially equivalent provisions can be identified under UK law.
104. In the draft decision, the European Commission reports explanations from the UK authorities according to which under common law or statutes, a foreign judgment requesting data is unenforceable in the UK without an international agreement and any transfer of data upon request from a foreign court or administrative authority requires a transfer tool such as an adequacy regulation or appropriate safeguards, unless a derogation under Article 49 UK GDPR applies. However, the EDPB has not been provided with the exchanges between the European Commission and the UK authorities⁶⁹ in this regard, and is therefore not able to analyse and independently assess

⁶⁴ See WP254 rev.01, p. 6.

⁶⁵ See WP254 rev.01, p. 6.

⁶⁶ See Article 44 GDPR, last sentence, in particular: “*All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*”

⁶⁷ See *Schrems I*, para. 91.

⁶⁸ See the annex to the EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, adopted on 10 July 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

⁶⁹ See footnote 78 of the draft decision.

whether the guarantees provided by the UK authorities are sufficient to ensure an essentially equivalent level of protection in relation to the safeguards contained in Article 48 GDPR.

105. **The EDPB invites the European Commission to provide further assurances and specific references to UK legislation that ensure that the level of protection under the UK legal framework is essentially equivalent to that guaranteed within the EEA. Therefore, the EDPB invites the European Commission to provide written explanations and commitments from the UK authorities with regard to the implementation of protections essentially equivalent to those provided by Article 48 GDPR.**
106. **The EDPB considers that the identification of provisions under UK law ensuring an essentially equivalent level of protection in relation to the safeguards contained in Article 48 GDPR is all the more important in light of the concerns previously raised concerning requests for access to data in the UK made by US or other third countries' authorities, and considering that as per the adequacy decision, personal data could be transferred from the EEA to the UK without any further guarantee or binding commitment from the recipient in relation to requests for access to data by other third countries' authorities.**

3.2. Procedural and Enforcement Mechanisms

107. Based on the criteria set forth in the GDPR Adequacy Referential, the EDPB has analysed the following aspects of the UK Data Protection Framework as covered under the draft decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance; and a system of access to appropriate redress mechanisms equipping individuals in the EU with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.

3.2.1 Competent Independent Supervisory Authority

108. The EDPB welcomes the efforts of the European Commission to examine comprehensively the establishment, functioning and powers of the UK supervisory authority in Chapter 2.6. of the draft decision. In the UK, the Information Commissioner (hereinafter "IC") is tasked with the oversight and enforcement of the compliance with the UK GDPR and the DPA 2018. According to Schedule 12 DPA 2018, the IC is a "Corporation Sole", i.e. a separate legal entity constituted in a single person, supported by an office, the ICO.
109. With regard to the independence of the IC, the EDPB underlines that Article 51 UK GDPR does not contain the express clarification that the IC is an independent public authority as it is stated in Article 51 GDPR with regard to SAs. The EDPB nevertheless acknowledges, that the UK GDPR mirrors in its Article 52 in a similar manner the corresponding rules with regard to the independence as set forth in Article 52(1) to (3) GDPR.
110. Furthermore, the EDPB points out that Article 52 UK GDPR does not hold obligations corresponding to Article 52(4) to (6) GDPR that expressly ensure that the respective SA is provided with resources necessary for the effective performance of its tasks and exercise of its powers. The EDPB however recognises that the DPA 2018 contains provisions which aim to secure an appropriate funding of the ICO⁷⁰, as well as the circumstance that the ICO is currently one of the largest SA compared to SAs within the EU/EEA. Since an ongoing allocation of appropriate resources, especially with regard to staff and budget⁷¹, is imperative so as to ensure the proper functioning of a SA to fulfil all of its

⁷⁰ See sections 137, 138, 182 and Schedule 12 para. 9 DPA 2018.

⁷¹ See WP 254 rev.01, p. 7.

assigned tasks and it has also been recently flagged by the European Parliament to be of major importance⁷², the EDPB deems it essential to pay particular attention to future developments in this area.

111. **Therefore, the EDPB invites the European Commission to observe any developments with regard to the allocation of resources to the ICO, which would be detrimental to the proper fulfilment of the ICO's tasks.**

3.2.2. Existence of a data protection system ensuring a good level of compliance

112. The draft decision undertakes a comprehensive examination of the powers that the ICO is equipped with under Article 58 UK GDPR and the DPA 2018 in order to ensure the monitoring and enforcement of the legislation. The EDPB acknowledges that Article 58 UK GDPR mirrors in a close manner the corresponding rules with regard to powers of SAs as set forth in Article 58 GDPR. Regarding the power to impose administrative fines depending on the circumstances of each individual case, Article 83 UK GDPR contains similar provisions and maximum amounts as set forth in Article 83 GDPR. Hence, the EDPB considers the UK legal framework in this field currently to be in line with the standards as set forth in the relevant law of the EU. In that respect, the EDPB nevertheless highlights that the existence of *effective* sanctions plays an important role in ensuring respect for rules.⁷³
113. **In the light of the above, the EDPB invites the European Commission to monitor the effectiveness of sanctions and relevant remedies in the UK Data Protection Framework.**

3.2.3. The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms

114. An effective supervision mechanism, allowing independent investigation of complaints so as to identify and punish infringements of data subject rights in practice, as well as an effective administrative and judicial redress (including compensation for damages as a result of the unlawful processing of data subject's personal data), are key elements for the assessment of whether a data protection system provides an adequate level of protection.
115. The EDPB welcomes that the ICO provides comprehensive information and guidelines on its website, which aim to raise awareness among controllers and processors in relation to their obligations and duties, as well as to support data subjects in order to be informed about their personal data rights and to assert their individual rights under the UK GDPR and the DPA 2018.
116. **Notwithstanding the current state, the EDPB invites the European Commission to continuously observe the level of support the ICO provides specifically to individuals, whose personal data have been transferred to the UK under the adequacy decision, to help them exercise their rights under the UK data protection regime.**

⁷² European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, para. 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_EN.html.

⁷³ See WP 254 rev.01, p. 7.

4. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EU BY PUBLIC AUTHORITIES IN THE UK

4.1. Access and use by UK public authorities for criminal law enforcement purposes

4.1.1. Legal bases and applicable limitations/safeguards

117. Regarding the assessment performed by the European Commission and documented in recitals 132 and following of the draft decision **on access for law enforcement purposes**, the European Commission provides nuanced and detailed information, and generally reaches comprehensible conclusions. Therefore, the EDPB refrains from reproducing most of the factual finding and assessments in this opinion. There are, however, certain instances where the depiction of the facts or the explanation of the conclusions do not suffice in order for the EDPB to espouse them.

4.1.1.1. The use of consent

118. The EDPB takes note that the European Commission asserts in footnote 184 of the draft decision⁷⁴ that **the use of consent** is not relevant in an adequacy scenario, as in transfer situations the data are not directly collected from a data subject by a UK law enforcement authority on the basis of consent. Consequently, the use of consent as a legal basis in policing is not assessed by the European Commission.
119. In this regard, the EDPB recalls that Article 45(2)(a) GDPR requires assessing a broad array of elements not limited to the transfer situation, including *“the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including [...] criminal law”*.
120. The EDPB notes, based also on the information provided by the European Commission in recital 38 of its draft implementing decision pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the UK (hereinafter “draft LED adequacy decision”), that the use of consent, as framed in the UK regime in the context of law enforcement, would always require a legal basis to be relied upon. This means that even if the police have statutory powers to process the data for the purpose of an investigation, in certain specific circumstances (for example to collect a DNA sample), the police may consider appropriate to ask for the consent of the data subject.
121. **The EDPB invites the European Commission to introduce in the adequacy decision its analysis on the possible use of consent in a law enforcement context, provided for in the draft LED adequacy decision.**

4.1.1.2. Search warrants and production orders

122. While the EDPB has no comments on the retrieval of evidence by the police through search warrants and production orders in general, it stems from recital 136 of the draft decision that the European Commission has centred its law enforcement access considerations around the police, and that the processing of personal data by other law enforcement agencies was less examined.

⁷⁴ See p. 37 of the draft decision.

123. For example, the UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement⁷⁵, suggests on p.11 that **the National Crime Agency** (hereinafter “NCA”) could be a law enforcement agency of particular interest, which *inter alia* has a wider criminal intelligence function. The NCA describes its mission as bringing together intelligence from a range of sources in order to maximise analysis, assessment and tactical opportunities, including from technical interception of communications, law enforcement partners in the UK and overseas, security and intelligence agencies⁷⁶. The NCA is also one of the main interlocutors for the international law enforcement partners, and plays a key role in the exchange of criminal intelligence⁷⁷.
124. The EDPB further takes note of the fact that the Government Communications Headquarters (hereinafter “GCHQ”), whose activities typically fall under the scope of Part 4 DPA 2018, i.e. national security, assumes as well an active role in reducing the societal and financial harm which serious and organised crime causes to the UK, working closely with the Home Office, NCA, HM Revenue and Customs (“HMRC”), and other government departments⁷⁸. Its activities relate to countering child sexual abuse; fraud; other types of economic crime, including money laundering; criminal use of technology; cybercrime; organised immigration crime, including people trafficking; and drugs, firearms and other illicit smuggling activity.
125. **The EDPB calls on the European Commission to complement its analysis with an analysis of the agencies active in the field of law enforcement that seem to have made collecting and analysing data, including personal data, a focus of their day-to-day operations, in particular the NCA. In addition, the EDPB invites the European Commission to have a closer look into the agencies like the GCHQ, whose activities fall both within the scope of law enforcement and national security, and the legal framework applicable to them for the processing of personal data.**

[4.1.1.3. Investigatory powers for law enforcement purposes](#)

126. Under Chapter 4 the GDPR Adequacy Referential ‘Essential guarantees in third **countries for law enforcement** and national security access to limit interferences to fundamental rights’, the EDPB recalls that “[i]n this context, the court also noted critically that the previous Safe Harbor decision did

⁷⁵ See UK Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 March 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F - Law Enforcement.pdf.

⁷⁶ See National Crime Agency’s website, Intelligence: enhancing the picture of serious organised crime affecting the UK, <https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk>.

⁷⁷ While not all intelligence processed by the NCA is personal data, a substantial portion might be personal information and the activities here described differ from those of classic policing, so that an assessment of access to personal data by law enforcement in the UK would be incomplete without thoroughly assessing the activities of the NCA. It seems reasonable to make sure that data protection principles are awarded the same meaning across all relevant law enforcement agencies, therefore shedding light on an especially data-driven agency such as the NCA. In addition, in “looking to the future”, the explanation continues, “[w]e continuously look for new opportunities to collect, develop and enhance traditional capabilities to increase the quantity and quality of intelligence available to exploit both in the UK and abroad.” “As part of this we are developing the new National Data Exploitation Capability, using the powers vested in the agency by the Crime and Courts Act, to link together, access and exploit data held across government.” [...] “All of this will increase our agility and flexibility to respond to new threats and operate in a proactive way, to gather and analyse information and intelligence on emerging threats so that we can take action before threats are realised.”

⁷⁸ See GCHQ’s website, Mission, Serious and Organised Crime, <https://www.gchq.gov.uk/section/mission/serious-crime>.

*"not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorized to engage in when they pursue legitimate objectives, such as national security."*⁷⁹. In this Referential, the EDPB states that the **four European Essential guarantees**⁸⁰ need to be respected for access to data, whether for national security purposes or for law enforcement purposes, by all third countries in order to be considered adequate, in particular the necessity and proportionality with regard to legitimate objectives pursued need to be demonstrated.

127. Under this section of the draft decision, the European Commission concludes (recital 139) "*since investigatory powers provided by the IPA 2016 are the same as those available to national security agencies, the conditions, limitations and safeguards applicable to such powers are addressed in detail in the Section on access and use of personal data by UK public authorities for national security purposes*". However it stems from the case-law of the CJEU, when applying the necessity and proportionality test to Member States' legislation allowing for retention and access to personal data by public authorities, that legitimate objectives, such as national security or fighting serious crimes, are different and, therefore, one might be able to justify a certain type of interference while the other might not⁸¹.
128. **The EDPB would therefore welcome a specific assessment within the decision of the necessity and proportionality of the conditions, limitations and safeguards described under recitals 174 and following - which is a section devoted to measures pursuing national security objectives - when it comes to applying these conditions, limitations and safeguards in the context of a measure pursuing a law enforcement objective. It thus invites the European Commission to further clarify whether the described retention of personal data and access to it for law enforcement purposes are sufficiently limited, so as to ensure an essentially equivalent level of protection to that guaranteed within the EU.**

[4.1.2. Further use of the information collected for law enforcement purposes \(recitals 140-154\)](#)

129. The EDPB notes that the UK Data Protection Framework provides for similar safeguards and limitations than the ones provided under EU law in relation to the further use of the information collected for law enforcement purposes.

[4.1.2.1. Further use for other law enforcement purposes](#)

130. The DPA 2018 indeed provides that personal data collected by a competent authority for a law enforcement purpose may be further processed (whether by the original controller or by another controller) for any other law enforcement purpose, provided that the controller is authorised by law to process data for the other purpose, and the processing is necessary and proportionate to that purpose. The European Commission notes that all the safeguards provided by Part 3 DPA 2018 apply to the processing carried out by the receiving authority. The EDPB highlights however that, under Part 3 DPA 2018, sections 44(4), 45(4), 48(3) and 68(7) provide for the possibility to restrict the rights of data subject, and section 79 provides for the possibility of issuing certificates attesting that a

⁷⁹ See WP254 rev.01, p.9.

⁸⁰ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

⁸¹ See CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, ECLI:EU:C:2020:791.

restriction is a necessary and proportionate measure to protect national security. The EDPB therefore recommends that the European Commission further assess the possible impact of such restrictions to the level of protection of personal data in relation to the further use of the information collected. Similarly, further clarification should also be provided in relation to the UK legal framework allowing for such onward sharing, in particular the Digital Economy Act 2017, as well as the Crime and Courts Act 2013 that allows for the sharing of information with the NCA.

4.1.2.2. Further use for other purposes than law enforcement within the UK

131. The DPA 2018 also provides that personal data collected for any law enforcement purpose may be processed for a purpose that is not a law enforcement one when the processing is authorised by law. In this case, the legal basis authorising such sharing is section 19 Counter-Terrorism Act 2008. In this regard, the EDPB notes that the scope and provisions of section 19 Counter-Terrorism Act is not fully addressed in the European Commission's assessment, and may imply further use of a broader nature, in particular as regards section 19(2) which provides that "*[i]nformation obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.*"
132. The EDPB also notes that the European Commission's reference to the fact that competent authorities are public authorities that must act in compliance with ECHR, including Article 8 thereof, thus ensuring that all data sharing between the law enforcement agencies and the intelligence services complies with data protection legislation, and with the ECHR, could be further substantiated by identifying the relevant acts and laws under the UK legal order laying down clearly and precisely such limits.

4.1.2.3. Further use in the context of onward transfers outside the UK

133. While the European Commission has referred to the fact that the UK-US CLOUD Act Agreement may affect onward transfers to the US from CSPs in the UK, the EDPB also highlights that the entry into force of this agreement may also affect the further use of the information collected through onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 UK-US CLOUD Act Agreement.
134. More broadly, the EDPB considers that the conclusion of future bilateral agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, may also significantly affect the conditions for further use of the information collected, since such agreements may affect the UK Data Protection Framework as assessed. The EDPB therefore recommends that the European Commission further assess this point, identifying the existence of international agreements, and clarifies whether the provisions of these agreements may affect the application of UK data protection law and provide for further limitation or exemption in relation to the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive assessment of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure and further use.

4.1.3. Oversight

135. The EDPB notes that the oversight of criminal law enforcement agencies is ensured by a combination of different Commissioners, in addition to the ICO. The draft adequacy findings mention the IPC, the Commissioner for the Retention and Use of Biometric Material, as well as the Surveillance Camera Commissioner. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight. Of particular importance on questions of access to personal data transferred

to the UK is the IPC. The understanding of the EDPB is that the IPC is a so-called “judicial commissioner”, as other judicial commissioners, to be referred to in the context of the national security chapter, and that those judicial commissioners enjoy the independence of judges, also when serving as commissioners. As to the office of the IPC, the European Commission explains in recital 245 of the draft decision that it functions independently as a so-called “arm’s length body”, while being funded by the Home Office.

136. The EDPB has not found in the draft decision further indication to assess the independence of the Commissioner for the Retention and Use of Biometric Material, as well as of the Surveillance Camera Commissioner.
137. **The European Commission is invited to further assess the independence of the judicial commissioners, also in cases where the Commissioner is not (anymore) serving as a judge, as well as to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and of the Surveillance Camera Commissioner.**

4.2. General legal framework on data protection in the field of national security

4.2.1. National security certificates

138. According to section 111 DPA 2018, controllers may apply for national security certificates issued by a Minister, member of the Cabinet, the Attorney general or the Advocate General for Scotland, certifying that exemptions from obligations and rights enshrined in Parts 4 to 6 DPA 2018 are a necessary and proportionate measure for the protection of national security. These certificates are meant to give controllers greater legal certainty, and will be conclusive evidence of the fact that national security is applicable when processing personal data. However, it should be mentioned that these certificates are not required in order to rely on national security exemptions, but instead are a measure of transparency⁸².
139. The EPDB understands from Schedule 20 DPA 2018, sections 17 and 18 that a national security certificate issued under the Data Protection Act 1998 (hereinafter “old certificate”) had an extended effect for the processing of personal data under the DPA 2018 until 25 May 2019. Until this date, unless replaced or revoked, the old certificates were treated as if they were issued under the DPA 2018.
140. However, where there is no express expiry date on a national security certificate issued under the Data Protection Act 1998, the EDPB understands that such a certificate will continue to have effect in relation to processing under the Data Protection Act 1998, unless the certificate is revoked or quashed⁸³. Even though the protection provided by these old certificates is limited to the processing of personal data under the Data Protection Act 1998, the EDPB takes note that new national security certificates can be issued under the Data Protection Act 1998 for personal data that was processed under the Data Protection Act 1998.⁸⁴

⁸² See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 4, p. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

⁸³ See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, p. 5.

⁸⁴ See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 8, p. 5.

141. **For the sake of comprehensiveness, the EDPB invites the European Commission to clarify in its draft decision that national security certificates can still be issued under the Data Protection Act 1998. Moreover, the EDPB invites the European Commission to describe in its draft decision the redress and oversight mechanisms with regard to certificates issued under the Data Protection Act 1998. Finally, the EDPB invites the European Commission to include in its draft decision the number of existing certificates issued under the Data Protection Act 1998, and to attentively monitor this aspect.**

4.2.2. Right to rectification and erasure

142. With regard to the right to rectification and erasure, the EDPB takes note that, in accordance with section 100 and section 149 DPA 2018, data subjects have the possibility to rely on the High Court (in Scotland, the Court of Session) to order a controller to rectify or delete their data without undue delay.
143. **The EDPB stresses that the exercise of data subjects' rights needs to be effectively ensured; therefore invites the European Commission to describe in its draft decision how section 100 DPA 2018 works in practice, and to closely monitor the application of this section.**

4.2.3. Exemptions for National Security

144. The EDPB wants to draw attention to section 110 DPA 2018, and in particular to Schedule 11, which sets out the specific purposes for which intelligence services can deviate from certain data protection principles, including in relation to data subjects' rights, and are not obliged to communicate personal data breaches to the ICO.⁸⁵
145. The **EDPB calls the European Commission to clarify further the scope of the exemptions as it wonders whether all of the exemptions provided under Schedule 11 DPA 2018 are relevant for the work of intelligence services, and whether they ensure the equivalence with the necessity and proportionality principle.** In particular, the EDPB invites the European Commission to provide more clarification under which circumstances an intelligence service could rely on section 10 of Schedule 11 DPA 2018, which states that "*[t]he listed provisions do not apply to personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject to the extent that the application of the listed provisions would be likely to prejudice the negotiations.*"

4.3. Access and use by UK public authorities for national security purposes

146. As a general remark, the EDPB acknowledges that States are granted a broad margin of appreciation in matters of national security, which is also recognised by the ECtHR. The EDPB also recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures⁸⁶, Article 6(3) Treaty on European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law. However, as the CJEU recalls in its jurisprudence,

⁸⁵ These purposes are the prevention and detection of "Crime", "Information required to be disclosed by law etc or in connection with legal proceedings", "Parliamentary privilege", "Judicial proceedings", "Crown honours and dignities", "Armed forces", "Economic well-being", "Legal professional privilege", "Negotiations", "Confidential references given by the controller", "Exam scripts and marks", "Research and statistics" and "Archiving in the public interest".

⁸⁶ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

the latter does not constitute, as long as the EU has not acceded to it, a legal instrument which has been formally incorporated into EU law⁸⁷. Thus, the level of protection of fundamental rights required by Article 45 GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the EU Charter. This being said, according to Article 52(3) EU Charter, the rights contained therein that correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR. Consequently, as recalled by the CJEU, the jurisprudence of the ECtHR concerning rights that are also foreseen in the EU Charter must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the EU Charter⁸⁸. According to the last sentence of Article 52(3) EU Charter, however, “[t]his provision shall not prevent Union law providing more extensive protection.”

147. Therefore, in the following assessment, the EDPB has taken into account the jurisprudence of the ECtHR, to the extent that the EU Charter, as interpreted by the CJEU, does not provide for a higher level of protection which prescribes other requirements than the ECtHR case-law.

[4.3.1. Legal bases, limitations and safeguards - Investigatory powers exercised in the context of national security](#)

[4.3.1.1. General remarks](#)

148. The EDPB recalls that the IPA 2016 is a recent law that amended several provisions of the Intelligence Services Act 1994. It sets out the extent to which certain investigatory powers may be used to interfere with privacy⁸⁹. Despite two reports of the IPC that provide useful information concerning the application of this new legal framework, there is still no review of certain aspects, in particular concerning the selectors and search criteria used.
149. Also, as a general remark concerning the IPA 2016 and its scope of application, the EDPB highlights the following four points of attention:
150. In relation to the **first point of attention**, with regard to the features of the law, the EDPB would like to underline two aspects:
151. First, the EDPB notes that the legislation refers to broad purposes for the use of procedures provided for in the IPA 2016 and not to the categories of individuals who may be concerned by the collection of data on the basis of Parts 2 to 7 IPA 2016. In this regard, the EDPB recalls that there should be a link between the categories of individuals who may be the subject of surveillance measures and the purposes pursued by the legislation to define the personal scope of the law.
152. Furthermore, the EDPB also stresses that the definition of “telecommunications operators”, “telecommunications service” and “telecommunications system”, which define the scope of the law, are also very broad and unclear to some extent. Indeed, the EDPB highlights that these notions, in the field of the IPA 2016, have to be understood in a much broader manner than under the telecommunications legislations, as defined for instance in the European Electronic Communications Code⁹⁰. The EDPB notes that the definitions of “telecommunications service” and

⁸⁷ See *Schrems II*, para. 98.

⁸⁸ See CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, ECLI:EU:C:2020:791, para. 124.

⁸⁹ See section 1 IPA 2016.

⁹⁰ See Article 2 (5) of the European Electronic Communications Code which defines, for instance, ‘interpersonal communications service’ as “a service normally provided for remuneration that enables direct

“telecommunication system” in the Act are said to be intentionally broad so that they will remain relevant for new technologies. Likewise, the definition of a telecommunications operator is also very broad, and could for instance include online videogames with a chat feature included, or other online websites merely including such chat windows⁹¹.

153. In addition, whereas procedures and oversight concerning the assessment of the necessity and proportionality of collection and access to data are generally provided, the criteria to proceed to such an assessment are not defined in the law itself. Additional elements can be found in other documents, such as Codes of practice.
154. However, as recalled in the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, the CJEU has indicated that “*the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned*”⁹². More precisely, the CJEU clarified that “[i]n order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and, in particular, must indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary.”⁹³
155. The ECtHR also stressed the importance of the clarity of the law to give individuals “*an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*”⁹⁴.
156. **The EDPB therefore calls on the European Commission to further assess these aspects concerning the preciseness, clarity and exhaustiveness of the relevant law, and to provide further elements to demonstrate it provides a level of protection essentially equivalent to that guaranteed within the EU with regard to the features of the law. The EDPB also stresses that broad definitions should also be assessed in relation to the proportionality of the interception measures.**
157. In addition, although several internal codes of the competent intelligence community authorities partly develop some of these elements, for instance concerning the assessment of the necessity and proportionality of collection of data, the EDPB stresses that the requirements of the CJEU in relation to the nature of the law imply that the core elements, including for individuals to be able to rely on

interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service”.

⁹¹ See Home Office, Code of practice on the interception of communications, March 2018, paras 2.5 and following,

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

⁹² See *Schrems II*, para. 175; and the case-law cited, as well as CJEU, case C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, 6 October 2020, ECLI:EU:C:2020:790 (hereinafter “Privacy International”), para. 65.

⁹³ See *Privacy International*, para. 68.

⁹⁴ See ECtHR, *Zakharov v. Russia*, 4 December 2015, CE:ECHR:2015:1204JUD004714306, para. 229.

them in the context of redress, must be provided in legislation providing for actionable rights⁹⁵. Indeed, Schedule 7, paragraph 6 IPA 2016 mentions the fact that courts (and supervisory authorities) “take into account a failure by a person to have regard to a code in determining a question in any such proceedings” without clarifying whether individuals can claim a breach of the codes before courts (or supervisory authorities). Moreover, the elements provided so far in the draft decision either refer to the recognition by the ECtHR of the foreseeability of the rules provided⁹⁶ in those codes, rather than to their “actionability” in court, as required by the CJEU, or to the fact that UK Courts have in some cases referred to codes, while none of the cases mentioned illustrate the possibility for individuals to action rights derived from the codes. **If it is concluded that UK law does not indicate sufficiently the circumstances and conditions under which a measure may be adopted and that these elements are in fact provided by internal codes of the intelligence community authorities, the EDPB would thus call on the European Commission to further assess whether the limitations and safeguards provided in the different internal codes of the intelligence community authorities may be actioned by individuals before a court and enforced.**

158. **The second point of attention** concerns the fact that the provisions relating to, on the one hand, targeted acquisition and retention of communications data and, on the other hand, to bulk collection, either in the IPA 2016 or in other legislations such as the Intelligence Services Act 1994, or the Regulation of Investigatory Powers Act 2000, will also apply to data transferred from the EU to the UK. Concerning bulk collection, the EDPB underlines that the relevant provisions of UK law allow for the collection of data outside the UK; thus could include data in transit transferred from the EEA to the UK on the basis of the adequacy decision⁹⁷. Moreover, the EDPB notices that the European Commission indicates that “[i]t should be noted that the retention and acquisition of communications data normally does not concern personal data of EU data subjects transferred under this Decision to the UK. The obligation to retain or disclose communications data pursuant to Part 3 and 4 of the IPA 2016 covers data that is collected by telecommunication operators in the UK directly from the users of a telecommunication service.”⁹⁸ Nevertheless, the EDPB highlights the lack of clarity concerning the fact that only establishments of these operators situated in the UK can receive requests from the competent UK authorities since the definition of telecommunications operator provided in section 261(10) IPA 2016 requires that “a telecommunications operator is a person who offers or provides a telecommunications service to persons in the UK or who controls or provides a telecommunication system which is (wholly or partly) in or controlled from the UK”. Consequently, personal data of EEA data subjects could actually be concerned, for instance in the case of data collected or generated by an establishment of a UK telecommunications operator located within the EEA, transferred to an establishment of this same operator situated in the UK on the basis of the adequacy decision (for commercial purposes), and then collected, within the UK, by the competent public authorities.

⁹⁵ In this regard, the CJEU considered for instance that PPD 28 in the US, did not qualify, although it provided also some limitations with regard to bulk collection, see *Schrems II*, para 181.

⁹⁶ See ECtHR, *Big Brother Watch and others v. the United Kingdom*, 13 September 2018, ECLI:CE:ECHR:2018:0913JUD005817013 (hereinafter “Big Brother Watch”), para. 325: “As the IC Code is a public document, subject to the approval of both Houses of Parliament, and has to be taken into account both by those exercising interception duties and by courts and tribunals, the Court has expressly accepted that its provisions could be taken into consideration in assessing the foreseeability of the RIPA regime.”

⁹⁷ See para 183 and following of *Schrems II* on the assessment of a legislation providing for access to data in transit between the EU and a third country in the context of an adequacy decision.

⁹⁸ See recital 196 of the draft decision.

159. **The EDPB is therefore of the view that the assessment of these provisions are also relevant for the assessment of the level of adequacy of the UK legal framework and calls on the European Commission to clarify this aspect, and further assess to what extent this is the case.** In particular, the EDPB calls on the European Commission to clarify its understanding of the scope of this legislation, including of what the notion of “users of telecommunications services” covers, and whether data from establishments of telecommunications operators outside the UK, to the extent that data of EEA data subjects are concerned, could be requested, given the very broad definition of telecommunications operators.
160. **The third point of attention** concerns the “double-lock” procedure. The EDPB notes that a new “double-lock” procedure has been introduced in the IPA 2016. Nonetheless, the EDPB also understands that even if, in principle, collection or access to data for national security or intelligence purposes can only take place with a warrant approved by a Judicial Commissioner, the IPA 2016 provides that *“in specific limited cases lawful interception without a warrant is possible and only prior authorisation by the competent IC authorities themselves is required [see infra section on Oversight], including for interceptions in accordance with overseas requests (section 52 of the IPA 2016)”*. As underlined hereafter, this also concurs to the concerns of the EDPB with regard, notably, to overseas disclosures. In addition, the EDPB also notes that for equipment interference, be it targeted or in bulk, a derogation to the double-lock procedure is also possible, and that the Judicial Commissioner is entitled to approve only the renewal of bulk warrants, after a maximum initial period of 6 months. **The EDPB calls on the European Commission to further assess and demonstrate that even in cases where the double-lock procedure does not apply, the UK legal framework provides for appropriate safeguards, including through the effective *ex post* oversight and redress possibilities offered to the individuals, to ensure that the level of protection provided is essentially equivalent to the one provided within the EU (see also infra section 4.3.3 on Oversight).**
161. Moreover, although the IPA 2016 has indeed introduced the “double-lock” procedure, the EDPB remains concerned with regard to certain features of the new legislation. Following the presentation of the corresponding sections of the draft decision, the EDPB has analysed the following types of collection and access to data in the same order as presented by the European Commission. The order of the elements assessed hereafter therefore does not reflect a hierarchy in terms of level of concern of the EDPB.

[4.3.1.2. Targeted acquisition and retention of communications data](#)

162. The EDPB notes that there are two officials who can grant targeted authorisations for obtaining communications data: the authorising officer in the Office for Communications Data Authorisations (hereinafter “the IPC”), a designated senior officer (a person holding a prescribed office or rank in a relevant public authority), in addition to the approval by a Judicial Commissioner in certain cases. However, it remains unclear for the EDPB, under the law and the relevant code, exactly which official authorises which type of targeted acquisition of communications data, and to what extent a designated officer would be sufficiently independent⁹⁹.
163. **The EDPB consequently calls on the European Commission to further assess this aspect and provide clearer explanations on these elements.**
164. Concerning the notice requiring the retention of communication data, the EDPB also notes that such notices can be addressed to a “description of operators”. This notion appears to mean that several

⁹⁹ See also infra concerning the assessment of the double-lock procedure and the independence of the Judicial Commissioner.

operators can be requested at the same time to all retain data. Indeed, the targeted nature of the acquisition does not relate to the number of operators, but to the name or description of persons, organisations, location or group of persons that constitute the “target”, a description of the nature of the investigation and a description of the activities for which the equipment is used. The EDPB therefore highlights that, depending on the number of operators concerned by such “description of operators”, the notice may be broader than what the procedure for targeted retention may seem to imply. **The EDPB invites the European Commission to further assess this aspect, and to provide further assurances that, even when notices are addressed to several operators, they remain limited to what is strictly necessary and proportionate.**

4.3.1.3. Equipment interference

165. The EDPB notes that “equipment interference” can derogate from the double-lock procedure in case of urgency¹⁰⁰. The EDPB is therefore concerned that the purposes for which such equipment interference can be required are broad, and that the criteria for urgency (in which case the Judicial Commissioner is not required to provide an *ex ante* authorisation following an assessment of the necessity and proportionality of the equipment interference) remain unclear. Since in the latter situation “the warrant ceases to have affect and may not be renewed” in case where the Judicial Commissioner does not approve the equipment interference *ex post*, the EDPB understands that the data collected meanwhile remain lawfully collected. For these data to be deleted, a specific order of the Judicial Commissioner may be issued¹⁰¹.
166. **The EDPB calls on the European Commission to further assess the conditions under which urgency can be invoked, and to provide clarifications concerning the possible avenues for the exercise of rights for the data subjects concerned, and possible redress avenues offered to them in the context of equipment interference operations, especially when they take place in the context of urgency leading to a derogation to the double-lock procedure.**

4.3.1.4. Bulk interception of data from bearers

167. As described in the report of the bulk powers review¹⁰² “[b]ulk interception typically involves the collecting of communications as they transit particular bearers (communication links).” The official IPA 2016 factsheet describes “bulk interception” as “the process for the collection of a volume of communications followed by the selection of specific communications to be read, looked at or listened to where it is necessary and proportionate.” The EDPB notes that “bulk interception” of data actually implies the collection of data even before any filtering by selectors (either simple in the context of the monitoring of individuals already known to pose a threat, or complex, in the context of the identification of new threats and of previously unknown persons of interest).
168. The acquisition of bulk communications data was also one of the issues examined by the CJEU in the Privacy International case, which resulted in a judgment of the Grand Chamber issued on 6 October 2020 (in addition to whether such collection of data was performed in the context of EU law, even for national security purposes). The IPA 2016 has replaced the legislation that was the subject of this judgment.
169. The EDPB notes that, with the introduction of the IPA 2016 in UK law, a warrant is now required also to intercept data in bulk. The process to issue this warrant relies on the determination of “operational purposes”. The list of these operational purposes is established by heads of intelligence services, and

¹⁰⁰ See section 109 IPA 2016.

¹⁰¹ See section 110, subsection 3, point b) IPA 2016.

¹⁰² See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016.

then approved by the Secretary of State. This decision is itself approved by an independent Judicial Commissioner who must review whether the warrant is necessary and proportionate to the operational purposes. The EDPB understands that the Judicial Commissioner does not have the power to assess the operational purposes themselves, but whether the warrant is necessary and proportionate to the operational purposes listed in the warrant. The Parliamentary Intelligence and Security Committee is provided with a copy of the list every three months, and the Prime Minister reviews the list of these operational purposes at least once a year.

170. However, on the basis of the elements provided by the European Commission in the draft decision, it appears difficult to assess the scope of these operational purposes provided in the list and whether the collection of data they allow meets the threshold set by the CJEU (for instance circumscribing the collection of data to a geographical area could be as narrow as a few streets, as well as collecting data from the EEA as a whole).
171. In addition, the EDPB underlines that data collected in bulk may be retained for long periods (to be available for further access for examination). Indeed, the EDPB notes that section 150, paragraphs 5 and 6 IPA 2016 provide only for the destruction of the copies of the data collected, and only if their retention is not necessary, or not likely to become necessary, in the interests of national security or any other grounds falling under the scope of section 138(2) IPA 2016, or if the retention is not necessary for several other purposes¹⁰³. The EDPB stresses that these grounds appear very broad, and in any case only copies of the data obtained are mentioned.
172. Furthermore, the EDPB also notes that in urgent cases, the IPA 2016 also allows for the modification of warrants without the prior-approval of a Judicial Commissioner, and that in such case, if the Judicial Commissioner consulted *ex post* within three working days after the modification refuses to approve the modification, the warrant should have effect as if the modification had not been made, but the data collected in-between remain collected lawfully¹⁰⁴. For these data to be deleted, a specific order of the Judicial Commissioner may be issued¹⁰⁵.
173. **The EDPB therefore calls on the European Commission for further clarifications and assessment of bulk interceptions, in particular on the selection and application of selectors in the context of these bulk interception procedures to clarify the extent to which access to personal data meets the threshold set by the CJEU (see also below section 4.3.1.7., in particular on the oversight on the selectors), and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data. An independent assessment from UK competent oversight authorities would be particularly useful.**
174. **The EDPB also underlines that it seems all the more critical that “overseas-related communications” which are within the scope of bulk interception practices appear to imply that data could be directly intercepted and collected in bulk within the EEA by the UK, including for data in transit between the EEA and the UK that would fall within the scope of the draft decision (see below section 4.3.2. on further use of the information collected for national security purposes and overseas disclosure).**

¹⁰³ See subsections 3 and 6 of section 150 IPA 2016.

¹⁰⁴ See section 147 IPA 2016 (Part 6, chapter I).

¹⁰⁵ See section 181, subsection 3, point b) IPA 2016.

4.3.1.5. Protection and safeguards for secondary data

175. In addition, the EDPB is concerned that the UK relevant legislation related to bulk interception does not provide for the same level of protection to all communications data. “Secondary data”, which can be obtained with a bulk warrant are, according to section 137 IPA 2016, both “systems data”, “which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise)”, and “identifying data”, “which is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise), is capable of being logically separated from the remainder of the communication, and if it were so separated, would not reveal anything of what might reasonably be considered to be the meaning (if any) of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication”¹⁰⁶.
176. The EDPB notes that these “secondary data”, also known as “metadata”¹⁰⁷, collected in bulk, seem not to benefit from the same safeguards as data collected with a targeted warrant, but also as content data collected in bulk. Indeed, the EDPB notices that the selection of any of the intercepted content benefits from more safeguards¹⁰⁸ than the selection of secondary data¹⁰⁹.
177. Furthermore, the EDPB stresses that both the ECtHR¹¹⁰ and the CJEU¹¹¹ have questioned the fact that such data are less sensitive than others, and in particular than content data. Indeed, the Code of Practice concerning interceptions presents as examples of “secondary data” (both “systems data” such as router configurations, email addresses or users ID; but also alternative account identifiers, as well as “identifying data”, such as the location of a meeting in a calendar appointment, photograph information, such as the time, date and location when it was taken). **The EDPB thus stresses the consistent assessment by the ECtHR and the CJEU, and recalls the concerns expressed in relation to secondary data that should benefit from specific safeguards due to their sensitivity. The EDPB**

¹⁰⁶ “Systems data” and “identifying data” are defined in section 263 IPA 2016.

¹⁰⁷ See Report of the bulk powers review, by the Independent Reviewer of Terrorism Legislation, August 2016.

¹⁰⁸ See section 152, subsection 1, point c) and subsections 3 and following IPA 2016.

¹⁰⁹ See section 152, subsection 1, points a) and b) IPA 2016.

¹¹⁰ See ECtHR, *Big Brother Watch*, para. 357, under referral to the Grand Chamber: “Consequently, while the Court does not doubt that related communications data is an essential tool for the intelligence services in the fight against terrorism and serious crime, it does not consider that the authorities have struck a fair balance between the competing public and private interests by exempting it in its entirety from the safeguards applicable to the searching and examining of content. While the Court does not suggest that related communications data should only be accessible for the purposes of determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands..”

¹¹¹ See CJEU, *Privacy International*, para. 71: “The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (see, by analogy, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 27 and 37, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 99 and 100).”

therefore calls on the European Commission to carefully assess whether the safeguards provided under UK law for such category of personal data ensure an essentially equivalent level of protection to the one guaranteed in the EU.

4.3.1.6. Automated processing of communications data

178. The EDPB notes that intelligence community authorities do not only use simple or complex selectors to filter the data acquired in bulk, but that they may also rely on other automated processing tools to analyse “*large volumes of information, which enables the Agencies also to find linkages, patterns, associations or behaviours which might demonstrate a serious threat requiring investigation*”, according to the Intelligence and Security Committee report 2015¹¹². **The EDPB is aware of the fact that this public report concerns practices under the previous legal framework, which was subsequently replaced by the IPA 2016. Nevertheless, it sees a need for further independent assessment and oversight of the use of automated processing tools by the competent UK oversight authorities, and calls on the European Commission to further assess this issue and the safeguards that would and/or could be afforded to EEA data subjects in this context.**

4.3.1.7. Compliance risks and incompliant practices of competent Intelligence Community authorities

179. The EDPB takes note that detailed oversight reports are available. They provide for valuable elements as to what they assess as positive compliance practices, as well as to the compliance risks and incompliant practices identified.
180. In this regard, according to the IPC in its report for 2019, several elements concerning the application of the legal framework by the different competent authorities have revealed some (risks of) incompliances by the competent authorities.
181. First, the EDPB has noticed that the criteria to classify a dataset as bulk personal dataset or as targeted data do not seem to be always clear for the MI5 and SIS themselves, in particular for the MI5, which can lead to the absence of appropriate safeguards applied to the data¹¹³. In its report on 2019, the IPC suggested that “*this question should be resolved as a priority*”¹¹⁴. Also in relation to bulk personal datasets, the EDPB notes that for the GCHQ, although the classification of bulk personal datasets seems to be satisfying (but yet remains to be audited by the IPC), in March 2019, the internal compliance review of warrants by the dedicated team raised serious concerns, with 50% of the justifications for bulk acquisition warrants that were reviewed by the GCHQ compliance team that did not meet the required standard. According to the IPC, the compliance team had begun work to

¹¹² See Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework, 2015, para. 18, p. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

¹¹³ See Annual Report of the Investigatory Powers Commissioner 2019, 15 December 2020, point 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: “*We have observed the positive development of the [Bulk Oversight Panel (BOP)] and note its impact in managing internal compliance. We continue to seek greater clarity regarding the process MI5 uses to carry out initial examinations of new data sets to better understand decisions to classify a dataset as BPD or, for example, as targeted data. We were concerned by one unresolved action on the BOP minutes around resolving discrepancies between allocations of BPD between MI5 and SIS. It is possible, because of the different uses of the data and the different cuts of data being held, that both agencies could hold the same dataset, or versions of it, and that it could lawfully be categorised as bulk by one and targeted data by the other. There is a risk that, if one of the agencies has incorrectly categorised the data holding as targeted then that data would be held without appropriate warrant and might not be subject to appropriate safeguards.*”

¹¹⁴ See Annual Report of the Investigatory Powers Commissioner 2019, point 8.39.

investigate the problem and retrain staff to improve this standard. The refreshed training on the IPA 2016 provisions and the additional training provided by policy and compliance networks (hereinafter “PCNs”) have improved GCHQ’s compliance in this area. The IPC does not expect to see a slip in this standard at future inspections, but will continue to review this area closely¹¹⁵. **The EDPB therefore shares the view that further review and monitoring of the said elements by the European Commission is needed as part of the assessment of the level of protection to ensure that this standard is improved, as underlined in the IPC’s report, and recalls that implementation and concrete application of the legal framework shall also be taken into account as provided under Article 45 GDPR when assessing the essential equivalence of a third country.**

182. More broadly, the EDPB stresses the points of attention shared by the IPC concerning the “task-based searches” led by the MI5 officers – which allows an investigator to conduct more than one search of the bulk personal data sets available to them, and the “*serious compliance risks associated with certain technology environments in use by MI5*”, concerning where data were stored in the environment, who had access to them, the extent to which they were being copied or shared, the deletion processes which applied to them, as well as concerning retention periods. Although the IPC indicates that measures have been taken and safeguards introduced, some of them remain manual and led on an individual, human-basis, it highlights that it is critical that the “*MI5 continues to maintain these new processes and to provide sufficient resources for them to function effectively. If MI5 identifies an increase in non-compliant behaviours*”¹¹⁶. The IPC expects they would be brought to its attention as soon as possible. **The EDPB therefore calls on the European Commission to closely monitor these aspects in the future.**
183. Concerning the GCHQ, the EDPB also understands from the report of the IPC that, for operations conducted under the bulk warrants, “*the quality of applications for internal approval was variable and we observed that there was room for improvement in the way that such applications were set out*”¹¹⁷, and that for targeted equipment interference, the explanations for the use of general descriptors were sometimes too general and imprecise¹¹⁸. The EDPB also noticed that in the context of bulk equipment interference, the IPC recommends that “*applications should consistently and explicitly record the link between the target and a statutory purpose and intelligence requirements*”¹¹⁹, that “*all applications should clearly address the potential for collateral intrusion and relevant mitigations when assessing proportionality*”¹²⁰, and that the IPC stressed that despite progress, “*there is still room for improvement*”¹²¹ and further attention will be needed as well in the future.
184. In relation to the bulk interception regime under the Regulation of Investigatory Powers Act 2000 (hereinafter “RIPA 2000”) which has since been replaced by provisions in the IPA 2016, the EDPB recalls that the insufficient oversight, both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, was one of the core aspects that the ECtHR deemed incompliant with Article 8 ECHR with regard to the previous legislation on the investigatory powers of UK authorities in the context of national security in the *Big Brother Watch* case, now referred to the Grand Chamber. **The EDPB invites the European**

¹¹⁵ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.48.

¹¹⁶ See Annual Report of the Investigatory Powers Commissioner 2019, point 8.52.

¹¹⁷ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.2.

¹¹⁸ See Annual Report of the Investigatory Powers Commissioner 2019, points 10.16 and 10.17.

¹¹⁹ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.

¹²⁰ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.

¹²¹ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.23.

Commission to verify the state of play of the proceedings, to take these elements into account, and to specify them in the adequacy decision should the European Commission adopt it.

185. In this case, the ECtHR was: “*not persuaded that the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination are sufficiently robust to provide adequate guarantees against abuse. Of greatest concern, however, is the absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications.*”¹²² As highlighted by the IPC, “*this finding echoed a similar recommendation in the Intelligence and Security Committee’s Privacy and Security: A modern and transparent legal framework report of March 2015*”¹²³. The EDPB welcomes the fact that consequently, the IPC conducted a review of its approach to inspecting bulk interception in 2019, “*which included a careful review of the technically complex ways in which bulk interception is actually implemented*”¹²⁴ and committed to include “*a detailed examination of the selectors and search criteria alluded to above by the ECtHR*”¹²⁵ in the inspections of bulk interception from 2020 onwards. Given the importance of this aspect, the EDPB is concerned that a detailed examination of the selectors and search criteria by the IPC has not been carried out yet, and calls on the European Commission to closely monitor developments in this regard, especially since the concrete format of such oversight remains to be clarified¹²⁶.

4.3.2. Further use of the information collected for national security purposes and overseas disclosure

186. When it comes to the further use of the information collected for national security purposes, the European Commission refers in its assessment to section 87(1) DPA 2018, which indeed provides that “*personal data so collected must not be processed in a manner that is incompatible with the purpose for which it is collected*”. The EDPB however points out that this provision may be subject to national security exemptions as per section 110 DPA 2018. The EDPB furthermore notes that, whether for targeted interception and examination, for targeted acquisition and retention of communications data, for targeted equipment interference or for bulk interception and bulk equipment interference, the legislation provides for the possibility of “overseas disclosure”.

4.3.2.1. Further use, overseas disclosure and the applicable legal framework in the UK

187. The European Commission has identified Part 4 DPA 2018, and in particular its section 109 as relevant provisions setting out specific requirements for the further use of the information collected, and notably the international transfer of personal data by intelligence services to third countries or international organisations. However, the EDPB notes that section 110 DPA 2018 provides for a national security exemption specifying that certain provisions of the DPA 2018 do not apply if exemption from these provisions is required for the purpose of safeguarding national security. The concerned provisions that may not apply include chapter 2 of Part 4 DPA 2018 in relation to the data protection principles, including purpose limitation, as well as chapter 3 of Part 4 DPA 2018 in relation to data subject rights. Section 109 DPA 2018, read in conjunction with section 110 DPA 2018 and the conditions under which it applies may lead to cases where an international transfer of personal data

¹²² See ECtHR, *Big Brother Watch*, para. 347.

¹²³ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.

¹²⁴ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.

¹²⁵ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28.

¹²⁶ See Annual Report of the Investigatory Powers Commissioner 2019, point 10.28: “the exact format of this inspection is yet to be agreed”.

by intelligence services to third countries takes place without applying provisions related to the data protection principles and data subject rights.

188. As identified by the European Commission, such exemption must be assessed case-by-case, and can be invoked only as far as the application of a particular provision would have negative consequences for national security. Indeed, the issuance of a national certificate for the UK intelligence services aims at certifying that an exemption is required in respect of specified personal data that are processed for the purpose of safeguarding national security. The EDPB however notes that in its guidance for national security certificate under the DPA 2018, the UK Home Office clarifies that “[i]t is important to note from the outset that a certificate is not required in order to rely on the national security exemption; in fact, in most cases, controllers will determine for themselves whether the national security exemption is applicable.”¹²⁷ Furthermore, the UK Home Office guidance notes that “national security certificates may apply to personal data which can be specifically identified or cover a broader category of personal data. They may be pre-emptive as well as retrospective.”¹²⁸ National security exemption may therefore apply in relation to an international transfer of personal data by intelligence services to third countries in the absence of a national security certificate.
189. The EDPB furthermore notes that, for example, the national security certificate DPA/S27/Security Service¹²⁹ provides that until 24 July 2024, personal data processed “*for, on behalf of, at the request of or with the aid or assistance of the Security Service or*” and “*where such processing is necessary to facilitate the proper discharge of the functions of the Security Service described in section 1 of the Security Service Act 1989*” are exempted from the corresponding provisions in UK law to Chapter V GDPR in relation to transfers of personal data to third countries or international organisations. While the other national security certificates publicly available do not provide for an exemption from the provisions of section 109 DPA 2018, it is to be recalled that some or all of the text of a national security certificate may be withheld if its publication would be against the interests of national security, would be contrary to the public interest, or might jeopardise the safety of any person.
190. In general, while assessing the draft decision in relation to these provisions, the EDPB observes that the safeguards for these disclosures solely comprise the requirement that the recipient of the data respects requirements concerning the security of data, the extent of the disclosure limited to what is necessary, the retention of data and the restriction of access to data to a limited number of persons. Thus, **the EDPB underlines that when it comes to overseas disclosures, the application of the national security exemption provided under UK law may lead to situations where safeguards ensuring that the principles of purpose limitation, necessity and proportionality, as well as the rights for the individuals, oversight and redress would not be fully provided or respected in the third country of destination. The EDPB therefore recommends the European Commission to further examine the overall safeguards provided under UK law when it comes to overseas disclosure, in particular in light of the application of national security exemptions.**

4.3.2.2. Overseas disclosure and intelligence sharing in the context of international cooperation

191. The EDPB also notes that the European Commission did not consider, as part of its adequacy assessment, existing international agreements concluded between the UK and third countries or

¹²⁷ See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 3, p. 3.

¹²⁸ See Home Office, The Data Protection Act 2018, National Security Certificates guidance, August 2020, para 5, p. 4.

¹²⁹ See DPA/S27/Security Service, section 27 DPA 2018, Certificate of the Secretary of State, 24 July 2019, <https://ico.org.uk/media/about-the-ico/documents/nscls/2615660/nsc-part-2-mi5-201908.pdf>.

international organisations that may provide for specific provisions for the international transfer of personal data by intelligence services to third countries.

192. The EDPB also stresses that the European Commission's assessment mainly relies on the assessment of Part 4 DPA 2018, and is notably concerned that the IPA 2016 focuses on 'requests' to exchange intelligence with foreign partners, but does not address other forms of intelligence sharing. The EDPB notes in this regard that the European Commission draft decision does not refer or assess the articulation between the UK legislative framework with the "UK-US Communication Intelligence Agreement" ("UK-US CI Agreement"). In a recent statement marking the 75th Anniversary of this agreement, the US National Security Agency (hereinafter "NSA") mentioned that this partnership allows "*to share information between the two agencies as much as possible, with minimal restrictions*" and that "*this ground-breaking document created the policies and procedures for UK and US intelligence professionals for sharing communication, translation, analysis, and code breaking information.*"¹³⁰ This agreement also became the foundation for other intelligence partnership with Australia, Canada, and New Zealand.
193. The secret nature of this agreement and its specific provisions raise a serious challenge in terms of clarity and foreseeability of the law in relation to the further use and overseas disclosure of information collected by UK authorities for national security purposes. In this context, the EDPB recalls that when it comes to the level of protection guaranteed within the EU, the CJEU has stressed that legislation involving interference with the fundamental right to the protection of personal data must "*lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data. The need for such safeguards is all the greater where personal data is subjected to automatic processing and where there is a significant risk of unlawful access to that data*"¹³¹. The EDPB therefore considers that the European Commission should consider the impact of the UK-US CI Agreement as part of its adequacy assessment.
194. The ECtHR, in its first section judgment of 13 September 2018, in the *Big Brother Watch* case, has assessed the UK intelligence sharing regime and in particular the UK-US CI Agreement. The ECtHR indeed stated that "*[t]he statutory framework which permits the United Kingdom intelligence services to request intercepted material from foreign intelligence agencies is not contained in RIPA. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permits the exchange of material between the United States and the United Kingdom*"¹³² and considered that there is "*a basis in law for the requesting of intelligence from foreign intelligence agencies, and that that law is sufficiently accessible.*"¹³³ While the ECtHR has concluded that there has been no violation of Article 8¹³⁴ ECHR in relation to the intelligence sharing regime, the EDPB notes that this judgment has now been referred to the Grand Chamber which decision is still pending. The EDPB also notes that in a partly concurring, partly dissenting opinion to this judgment, Judge Koskelo, joined by Judge

¹³⁰ See NSA's press release, GCHQ and NSA Celebrate 75 Years of Partnership, 5 February 2021, <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership>.

¹³¹ See *Schrems I*, para. 91.

¹³² See ECtHR, *Big Brother Watch*, para. 425.

¹³³ See ECtHR, *Big Brother Watch*, para. 427.

¹³⁴ See ECtHR, *Big Brother Watch*, para. 448.

Turković¹³⁵, has concluded that there is a violation of Article 8 ECHR in relation to the intelligence sharing regime, stating that “[i]t is easy to agree with the principle that any arrangement under which intelligence from intercepted communications is obtained via foreign intelligence services, whether on the basis of requests to carry out such interception or to convey its results, should not be allowed to entail a circumvention of the safeguards which must be in place for any surveillance by domestic authorities (see paragraphs 216, 423 and 447). Indeed, any other approach would be implausible”.

195. As highlighted by several reports from the media and non-governmental organisations¹³⁶¹³⁷, the most recent version of the UK-US CI Agreement to have been made public dates back from 1956 and since then, communication technology and the nature of signals intelligence have changed significantly. Media reports have for example revealed that data transiting through undersea cables that land in the UK are intercepted by the GCHQ and made accessible to the NSA¹³⁸.
196. For the EDPB, a key question in relation to intelligence sharing is whether section 109 DPA 2018 and the provisions of the IPA 2016 remain applicable when UK intelligence services act in accordance with the UK-US CI Agreement. Another key element to be assessed is whether the provisions or effective application of this agreement impact on the level of protection of personal data in transit from the EEA to the UK, or allows for a direct access and acquisition of personal data by other third countries intelligence services.
197. Consequently, in addition to reservations expressed as to “overseas disclosures” on the basis of Part 4 DPA 2018 and its related national security exemption, as well as of requests in the framework of the IPA 2016, **the EDPB is concerned about other forms of information-sharing and disclosures, on the basis of other instruments, in particular the various international agreements concluded by the UK with other third countries, especially where these instruments remain inaccessible to the public, such as the UK-US CI Agreement. The effect of such agreement could lead to a circumvention of the safeguards identified in relation to the access and use of personal data for national security purposes.**
198. Indeed, the EDPB shares the view expressed by Special Rapporteur to the United Nations, Joe Cannatacci, that “[i]ntelligence sharing must not result in a backdoor to obtain or facilitate for others the obtaining of intelligence free from domestic safeguards, nor a loophole for foreign Governments with lower standards on the protection of privacy (or other human rights) to obtain intelligence from UK intelligence that could give rise to human rights violations”¹³⁹.
199. Furthermore, **the EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purpose of intelligence cooperation, providing a legal basis for direct interception and acquisition of personal data or the transfer of personal data to these countries**

¹³⁵ See ECtHR, *Big Brother Watch*, partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković.

¹³⁶ See BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes, 5 March 2021, <https://www.bbc.com/news/uk-56284453>.

¹³⁷ See Privacy International, Policy Briefing - UK Intelligence Sharing Arrangements, April 2018, <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf>.

¹³⁸ See The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications, 21 June 2013, <https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa>.

¹³⁹ See End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland, London, 29 June 2018, <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give>.

may also significantly affect the conditions for further use of the information collected, since such agreements are likely to affect the UK data protection legal framework as assessed.

4.3.3. Oversight

200. The EDPB emphasises the importance of comprehensive supervision by independent supervisory authorities for an adequate level of data protection. The guarantee of independence within the meaning of Article 8(3) EU Charter of the supervisory authorities is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals with regard to the processing of personal data.
201. When personal data are accessed and used for national security purposes, the oversight function is mainly fulfilled by the IPC and the Judicial Commissioners (hereinafter the "Judicial Commissioners").
202. **The EDPB generally recognises the introduction of Judicial Commissioners in the IPA 2016 as a significant improvement.** In line with a request above, the European Commission is invited to assess the independence of the **Judicial Commissioners in more detail, and in particular to what extent the independence of the IPC and the IPC's office (hereinafter "IPCO") is legally secured, as such is not found in the IPA 2016.** This is even more important as the IPC decides on appeals by the government, in case an application for a surveillance **measure** has been denied **by** a judicial commissioner.
203. The IPC has *ex-ante*, as well as *ex-post* oversight functions. As regards *ex-ante* oversight, the EDPB understands that the function of the Judicial Commissioners is to approve, in individual cases, different surveillance measures, including targeted interception and bulk acquisition of communication data. The EDPB further notes that prior-approval of surveillance measures cannot be derived from the jurisprudence of the CJEU as an absolute requirement for the proportionality of surveillance measures.¹⁴⁰
204. In order to assess the effectiveness of this level of oversight, the EDPB nevertheless sees the need to further clarify the scenarios for which a lawful interception without a prior-approval of the Judicial Commissioners is possible.
205. In its draft decision, the European Commission mentions in footnotes 201 and 266 "specific limited cases" provided by the IPA 2016 in its sections 44 to 52 with regard to targeted interceptions. The EDPB notes that sections 45 - 51 IPA 2016 are exemptions that are claimed not to be regularly used by intelligence services. Furthermore, the **EDPB understands** that in the **cases where the exemptions apply** (e.g. telecommunications and postal providers), the prior-approval carried out by the Judicial Commissioners is to be conducted in the event that law enforcement authorities or intelligence services **request** access to these data, **and invites the European Commission to confirm in its decision that this is correct.**
206. The EDPB recognises that section 44(2) IPA 2016 permits interception of communications if one of the parties (sender or recipient) has consented and there is an authorisation under the RIPA 2000 or the Regulation of Investigatory Powers (Scotland) Act 2000 (2000 asp 11), i.e. the former legal situation before the establishment of the Judicial Commissioners. The EDPB **invites** the European

¹⁴⁰ It also notes, however, that the CJEU, when invalidating the Privacy Shield in *Schrems II*, has taken note of the fact that, under US law, the so called FISA Court "*does not authorise individual surveillance measures; rather, it authorises surveillance programs (like PRISM, UPSTREAM) on the basis of annual certifications*". (para. 179).

Commission to clarify whether this means that in cases where a unilateral consent exists, the prior-approval procedure would not apply at all.

207. As regards *ex-post* oversight, it is also important to verify that efficient independent oversight is ensured without gaps, in particular where it is not foreseen *ex-ante*.
208. The EDPB notes that for the sections 48 - 52 IPA 2016, an *ex-post* review by the Judicial Commissioners takes place, and **invites the European Commission to clarify under which requirements and on whose initiative such an *ex-post* review is to be conducted**.
209. According to section 229(4) IPA 2016, the IPC is not to keep under review the exercise of certain functions. In this regard the EDPB invites the European Commission to clarify the provisions of section 229(4)(d) and (e) IPA 2016 regarding its practical impact on the review competence of the IPC. **It is the understanding of the EDPB that the ICO is the competent oversight authority where the exemptions of section 229(4) IPA 2016 apply, and the EDPB invites the European Commission to confirm in its decision that this is correct.**
210. **It appears that, when conducting *ex-post* oversight, the IPC's role is limited to make recommendations in cases of non-compliance, and to give notice to the data subject, if the error is serious and it is in the public interest for the person to be informed. The EDPB invites the European Commission to clarify how the ICO can effectively ensure compliance with the law.**
211. **Finally, the EDPB understands that affected individuals cannot directly address the ICO, but must lodge a complaint with the ICO, which, however, has limited competences in the area of national security. The EDPB therefore invites the European Commission to further clarify how it is legally ensured that the ICO addresses complaints in these cases.**

4.3.4. Redress

212. In the light of the *Schrems I* and *Schrems II* judgments by the CJEU, it is clear that effective judicial protection in the meaning of Article 47 EU Charter is of fundamental importance for the assumption of adequacy of the law of a third country. The rulings have also shown that particular attention, in this regard, has to be paid to effective judicial protection in the area of national security access to personal data.
213. **The EDPB recognises that the UK has established the IPT. The IPT is not only competent to hear cases on the use of investigatory powers by law enforcement authorities, but also by intelligence services. It is the understanding of the EDPB that the IPT functions as a proper court in the meaning of Article 47 EU Charter. As to its powers, the European Commission is invited to confirm that the IPT has all those powers mentioned in recital 262 of the draft decision, regardless of the legal basis under which the complaint is brought.**
214. Discreet surveillance by intelligence agencies will often mean that the object of the surveillance, the data subject, is and will not be aware of the surveillance. In this context, when it had to analyse US law, the EDPB has many times expressed its concern with the requirement of "standing", as interpreted in US law, in surveillance cases. Against this background, the EDPB notes that the complaint with the IPT only requires a "belief" test, according to which the complainant has to show she or he is potentially at risk of being subjected to a measure.
215. When analysing the IPT, the EDPB also pays particular attention to the fact that the functioning of the IPT has been repeatedly found to be in compliance with the ECHR, as interpreted by the ECtHR.

**Opinion 15/2021 regarding the European Commission Draft
Implementing Decision pursuant to Directive (EU) 2016/680
on the adequate protection of personal data in the
United Kingdom**

Adopted on 13 April 2021

Version history

Version 1.1	06 July 2021	Formatting change
Version 1.0	13 April 2021	Adoption of the Opinion

CONTENTS

1	EXECUTIVE SUMMARY.....	4
2	INTRODUCTION	6
2.1	UK data protection framework	6
2.2	Scope of the EDPB's assessment	6
2.3	General comments and concerns.....	8
2.3.1	International commitments entered into by the UK.....	8
2.3.2	Possible future divergence of UK Data Protection Framework	8
3	RULES APPLYING TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE CRIMINAL LAW ENFORCEMENT PURPOSES.....	9
3.1	Material scope	9
3.2	Safeguards, rights and obligations	10
3.2.1	Processing on the basis of “consent” of the data subject.....	10
3.2.2	Individual rights	11
3.2.2.1	<i>National security certificates</i>	11
3.2.2.2	<i>LED Automated decision-making</i>	12
3.2.3	Onward transfers.....	12
3.2.4	Further processing, including onward sharing for national security purposes.....	14
3.3	Oversight and enforcement	15

The European Data Protection Board

Having regard to Article 51(1)(g) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA¹ (hereinafter “LED”),

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1 EXECUTIVE SUMMARY

1. The European Commission endorsed its draft implementing decision (hereinafter “draft decision”) on the adequate protection of personal data by the United Kingdom (hereinafter “UK”) pursuant to the LED on 19 February 2021². Following this, the European Commission initiated the procedure for its formal adoption.
2. On the same date, the European Commission asked for the opinion of the European Data Protection Board (hereinafter “EDPB”)³. The EDPB’s assessment of the adequacy of the level of protection afforded in the UK has been made on the basis of the examination of the draft decision itself, as well as on the basis of an analysis of the documentation made available by the European Commission.
3. The EDPB has used as main reference for this work its LED Adequacy Referential⁴ adopted on 2 February 2021, as well as the relevant case-law reflected in the EPDB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures⁵.
4. The EDPB’s key objective is to give an opinion to the European Commission on the adequacy of the level of protection afforded to individuals in the UK. It is important to recognise that the EDPB does not expect the UK legal framework to replicate European data protection law.
5. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 36 LED and the case-law of the Court of Justice of the European Union (hereinafter “CJEU”) require the third country’s legislation to be aligned with the essence of the fundamental principles enshrined in the LED. In the area of data protection, the EDPB notes that there is a strong alignment between the LED framework and the UK legal framework on certain core provisions such as, for example concepts (e.g., “personal data”; “processing of personal data”; “data controller”); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data

¹ OJ L 119, 4.5.2016, p. 89.

² See European Commission’s press Release, press release, Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

³ Idem.

⁴ See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, adopted on 2 February 2021, https://edpb.europa.eu/sites/edpb/files/files/file1/recommendations012021onart.36led.pdf_en.pdf.

⁵ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

- retention, security and confidentiality; transparency; special categories of data; automated decision making and profiling.
6. The EDPB recommends that the European Commission complement its analysis with information about the existence of a mechanism to inform the relevant Member States' competent authorities of further processing or disclosure by the UK authorities to which they transferred the personal data and identify its effectiveness under the UK legal order.
 7. The EDPB considers that the provisions under Chapter 5 of Part 3 Data Protection Act 2018 (hereinafter "DPA 2018"), do, in principle, provide for a level of protection that is essentially equivalent to the one guaranteed under EU law, when it comes to transfer of personal data from a UK law enforcement authority to a third country.
 8. Although the EDPB notes the capacity of the UK, under its legal framework, to recognise territories as providing an adequate level of data protection in light of the UK data protection framework, the EDPB wishes to highlight that this might lead to possible risks in the protection provided to personal data transferred from the EU especially if, in the future, the UK data protection framework deviates from the EU acquis. **For the above situations, the European Commission should therefore fulfil its monitoring role, and in case the essentially equivalent level of protection of personal data transferred from the EU is not maintained, the European Commission should consider amending the adequacy decision to introduce specific safeguards for data transferred from the EU, and/or to suspend the adequacy decision.**
 9. **Finally, regarding international agreements concluded between the UK and third countries,** the European Commission is invited to examine the interplay between the UK data protection framework and its international commitments, in particular to ensure the continuity of the level of protection where personal data are transferred from the EU to the UK on the basis of the UK adequacy decision, and then onward transferred to other third countries; and to continuously monitor and take action, where necessary, in the event that the conclusion of international agreements between the UK and third countries risks to undermine the level of protection of personal data provided for in the EU.
 10. In this regard, the EDPB highlights that the entry into force of the Agreement between the UK and the US on Access to Electronic Data for the Purpose of Countering Serious Crime (hereinafter "UK-US CLOUD Act Agreement")⁶ may affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act Agreement.
 11. The EDPB also recommends that the European Commission continuously monitors whether the conclusion of future agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, could affect the conditions for onward sharing of the information collected, in particular whether the provisions of these international agreements may affect the application of UK data protection law and provide for further limitation or exemption in relation to the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive review of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure.

⁶ See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019.

2 INTRODUCTION

2.1 UK data protection framework

12. The UK data protection framework is largely based on the EU data protection framework (in particular the LED and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter “GDPR”)), which derives from the fact that the UK was a Member State of the EU up until the 31 January 2020. Moreover, the DPA 2018, which came into force on 23 May 2018 and repealed the UK Data Protection Act 1998, transposes the LED through Part 3 thereof, in addition to further specifying the application of the GDPR in UK law, as well as granting powers and imposing duties on the national data protection supervisory authority, the UK Information Commissioner’s Office (hereinafter “ICO”).
13. As mentioned in recital 12 of the draft decision, the UK Government enacted the European Union (Withdrawal) Act 2018, which incorporates directly applicable EU legislation into the law of the UK. Under this Act, the ministers of the UK have the power to introduce secondary legislation, via statutory instruments, to make the necessary modifications to retained EU law following to the UK’s withdrawal from the EU to fit the domestic context.
14. Consequently, the relevant legal framework applicable in the UK after the end of the transition period⁷ consists of:
 - the United Kingdom General Data Protection Regulation (hereinafter “UK GDPR”), as incorporated into the law of the UK under the European Union (Withdrawal) Act 2018, as amended by the DPPEC (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019;
 - the DPA 2018, as amended by the DPPEC Regulations 2019, and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020; and
 - the Investigatory Power Act 2016 (“IPA 2016”).

(together “the UK Data Protection Framework”).

2.2 Scope of the EDPB’s assessment

15. The draft decision of the European Commission is the result of an assessment of the UK data protection framework, followed by discussions with the UK Government. In accordance with Article 51(1)(g) LED, the EDPB is expected to provide an independent opinion on the European Commission’s findings, identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these.
16. As mentioned in the LED Adequacy Referential, “*the information provided by the European Commission should be exhaustive and put the EDPB in a position to make an own assessment regarding the level of data protection in the third country*⁸”.

⁷ The transition period is set for 31 December 2020 after which date EU law no longer applies in the UK. The “bridge period” is set for 30 June 2021 at the latest and refers to the additional period during which transmission of personal data from the EU to the UK is not deemed a transfer.

⁸ See Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 15, p. 5.

17. In this regard, it is to be noted that the EDPB only partially received documents relevant for the examination of the UK legal framework on time. The EDPB received most part of the UK legislation referred to in the draft decision through links referenced in the latter. The European Commission was not in a position to provide the EDPB with written explanations and commitments from the UK in relation to the exchanges between the UK authorities and the European Commission relevant to this exercise⁹.
18. Taking into account the above and due to the limited timeframe (2 months) afforded to the EDPB to adopt this opinion, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them. When analysing the law and practice of a third country which has been a Member State of the EU until recently, it is evident that the EDPB has identified many aspects to be essentially equivalent. In view of its role in the process of adopting an adequacy finding and the amount of law and practice to be analysed, the EDPB has decided to focus its attention to those aspects where it saw the greatest need to look closer.
19. The EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the Charter of Fundamental rights of the European Union (hereinafter “the EU Charter”), respectively protecting the right to private and family life, the right to protection of personal data, and the right to an effective remedy and fair trial; and Article 8 of the European Convention on Human Rights (hereinafter “ECHR”) protecting the right to private and family life. In addition to the above, the EDPB considered the requirements of the LED, as well as the relevant case-law.
20. The objective of this exercise is to provide the European Commission with an opinion for the assessment of the adequacy of the level of protection in the UK. The concept of “adequate level of protection”, which already existed under Directive 95/46/EC, has been further developed by the CJEU. It is important to recall the standard set by the CJEU in *Schrems I*, namely that – while the “level of protection” in the third country must be “essentially equivalent” to that guaranteed in the EU – “the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU”¹⁰. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but

⁹These are the elements where the European Commission refers, in its draft decision, to explanations from the UK authorities without providing the written documents from the UK authorities supporting the explanations, such as with regard to: the effects of the transitional provisions and the absence of a “sunset” provision (recital 87); examples of consent as an appropriate basis for the processing (footnote 68); the term “inaccurate” as “incorrect or misleading” personal data (footnote 79); the remit of ISC (footnote 245); the low threshold for making a complaint with the IPT and the fact that it is not unusual for the IPT to determine that the complainant was in fact never subject to investigation by a public authority (footnote 263); the combination of powers derived from the legislation and common law (footnote 52); the prerogative powers exercised by the government (footnote 62); the fact that other organisations are free to follow the MoPI Code of Practice principles if they wish (footnote 86).

¹⁰See CJEU, C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650 (hereinafter “*Schrems I*”), paras. 73-74.

also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules¹¹.

2.3 General comments and concerns

2.3.1 International commitments entered into by the UK

21. According to Article 36 (2) (c) LED and the LED Adequacy Referential¹², when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems in particular in relation to the protection of personal data, as well as the implementation of such obligations. Furthermore, the third country's accession to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to the Automatic Processing of Personal Data (hereinafter "Convention 108")¹³ and its Additional Protocol¹⁴ should be taken into account.
22. **In this regard, the EDPB welcomes that the UK has adhered to the ECHR and is under the jurisdiction of the European Court of Human Rights ("ECtHR"). In addition, the UK has also adhered to Convention 108 and its Additional Protocol, has signed Convention 108+¹⁵ in 2018 and is currently working on its ratification.**

2.3.2 Possible future divergence of UK Data Protection Framework

23. As mentioned in recital 171 of the draft decision, the European Commission must take into account that, with the end of the transition period provided by the Withdrawal Agreement¹⁶, the UK administers, applies and enforces its own data protection regime and as soon as the bridge provision¹⁷ under Article FINPROV.10A of the EU-UK Trade and Cooperation Agreement¹⁸ ceases to apply, this may notably involve amendments or changes to the data protection framework assessed in the draft decision, as well as other relevant developments.

¹¹ See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para. 14, p. 5.

¹² See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 24, p.7.

¹³ See Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Convention 108, 28 January 1981.

¹⁴ See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, opened for signature on 8 November 2001.

¹⁵ See Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention 108+"), 18 May 2018.

¹⁶ See Agreement on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (OJ L 029, 31.1.2020, p. 7).

¹⁷ The transition period is set for 31 December 2020, after which date EU law no longer applies in the UK. The "Bridge period" is set for 30 June 2021 at the latest, and refers to the additional period during which transmission of personal data from the EU to the UK is not deemed a transfer.

¹⁸ See Trade and cooperation agreement between the European union and the European atomic energy community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (OJ L 444, 31.12.2020, p. 14).

- 24. The European Commission has therefore decided to include a sunset clause in its draft decision¹⁹, setting the expiration date four years after its entry into force.
- 25. It is important to note that the possibility of the UK ministers and the UK Secretary of State to introduce secondary legislation following the end of the bridge period may lead to a significant divergence of the UK Data Protection Framework from the EU's in the future.
- 26. Finally, not only since the end of the transition period, the UK is no longer bound by CJEU case-law but also, the already adopted judgments of the CJEU, considered as retained case law in the UK legal framework, might not bind the UK any more as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period and its Supreme Court is not bound by any retained EU case-law²⁰.
- 27. **Considering the risks related to the possible deviation of the UK Data Protection Framework from the EU acquis following the end of the bridge period, the EDPB welcomes the European Commission's decision to introduce a sunset clause of four years for the draft decision. However, the EDPB would like to highlight here the importance of the European Commission's monitoring role²¹. Indeed, the European Commission should monitor all relevant developments in the UK that may have an impact on the essential equivalence of the level of protection of personal data transferred under the UK adequacy decision on an ongoing and permanent basis from its entry into force. In addition, the European Commission should take appropriate action by suspending, amending or repealing the adequacy decision, based on the circumstances at hand, if after the adequacy decision is adopted, the European Commission has indications that an adequate level of protection is no longer ensured in the UK.**
- 28. On its side, the EDPB will use its best efforts to inform the European Commission about any relevant action undertaken by Member State's Data Protection Supervisory Authorities (hereinafter "SAs"), and in particular regarding complaints made by data subjects in the EU concerning the transfer of personal data from the EU to the UK.

3 RULES APPLYING TO THE PROCESSING OF PERSONAL DATA BY COMPETENT AUTHORITIES FOR THE CRIMINAL LAW ENFORCEMENT PURPOSES

3.1 Material scope

- 29. In relation to recitals 24 and following of the draft decision, the EDPB notes that the draft adequacy decision does not contain much details on the activities and legal framework applicable to agencies other than the police having law enforcement duties.
- 30. For example, the UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement²², suggests on page 11 that **the National Crime Agency** (hereinafter "NCA") could be a law enforcement

¹⁹ See Article 4 of the draft decision. See also recital 172 of the draft decision.

²⁰ See section 6(3) to (6) EU (Withdrawal) Act 2018.

²¹ See Article 36(4) LED.

²² See UK Government, Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement, 13 March 2020.

agency of particular interest, which *inter alia* has a wider criminal intelligence function. The NCA describes its mission as bringing together intelligence from a range of sources in order to maximise analysis, assessment and tactical opportunities, including from technical interception of communications, law enforcement partners in the UK and overseas, security and intelligence agencies²³. The NCA is also one of the main interlocutors for the international law enforcement partners and plays a key role in the exchange of criminal intelligence²⁴.

31. The EDPB further takes note of the fact that the Government Communications Headquarters (hereinafter “GCHQ”), whose activities typically fall under the scope of Part 4 DPA 2018, i.e. national security, assumes as well an active role in reducing the societal and financial harm which serious and organised crime causes to the UK, working closely with the Home Office, NCA, HM Revenue and Customs (“HMRC”), and other government departments²⁵. Its activities relate to countering child sexual abuse, fraud, other types of economic crime, including money laundering, criminal use of technology, cybercrime, organised immigration crime, including people trafficking, and drugs, firearms and other illicit smuggling activity.
32. **The EDPB calls on the European Commission to complement its analysis with an analysis of the agencies active in the field of law enforcement that seem to have made collecting and analysing data, including personal data a focus of their day-to-day operations, in particular the NCA. In addition, the EDPB invites the Commission to have a closer look into the agencies like the GCHQ, whose activities fall both within the scope of law enforcement and national security, and the legal framework applicable to them for the processing of personal data.**

3.2 Safeguards, rights and obligations

3.2.1 Processing on the basis of “consent” of the data subject

33. The EDPB takes note that the European Commission asserts in recitals 37 and 38 of the draft decision that **the reliance on consent** is not considered relevant in an adequacy scenario, as in transfer situations the data are not directly collected from a data subject by a UK law enforcement authority on the basis of consent.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F-Law-Enforcement.pdf.

²³ See National Crime Agency’s website, Intelligence: enhancing the picture of serious organised crime affecting the UK, <https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk>.

²⁴ While not all intelligence processed by the NCA is personal data, a substantial portion might be personal information and the activities here described differ from those of classic policing, so that an assessment of access to personal data by law enforcement in the UK would be incomplete without thoroughly assessing the activities of the NCA. It seems reasonable to make sure that data protection principles are awarded the same meaning across all relevant law enforcement agencies, therefore shedding light on an especially data-driven agency such as the NCA. In addition, in “looking to the future”, the explanation continues, “[w]e continuously look for new opportunities to collect, develop and enhance traditional capabilities to increase the quantity and quality of intelligence available to exploit both in the UK and abroad.” “As part of this we are developing the new National Data Exploitation Capability, using the powers vested in the agency by the Crime and Courts Act, to link together, access and exploit data held across government.” [...] “All of this will increase our agility and flexibility to respond to new threats and operate in a proactive way, to gather and analyse information and intelligence on emerging threats so that we can take action before threats are realised.”

²⁵ See GCHQ’s website, Mission, Serious and Organised Crime, <https://www.gchq.gov.uk/section/mission/serious-crime>.

34. In this regard, the EDPB recalls, that Article 36(2)a) LED requires assessing a broad array of elements not limited to the transfer situation, including “*the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including [...] criminal law*”.
35. Consent in the law enforcement context can be relevant as a legal basis for data processing, as an additional safeguard, or more generally as a basis to execute investigative powers that lead to the acquisition of personal data, for example the consent of a third party to search their premises, or to confiscate data storage.
36. The EDPB notes, based also on the information provided by the European Commission in recital 38 of the draft decision, that the use of consent, as framed in the UK regime, would always require a legal basis to be relied upon. This means that even if the police have statutory powers to process the data for the purpose of an investigation, in certain specific circumstances (for example to collect a DNA sample), the police may consider appropriate to ask for the consent of the data subject.
37. **The EDPB invites the European Commission to analyse, as a rule, the possible use of consent in a law enforcement context when assessing the adequacy of a third country under the LED.**

3.2.2 Individual rights

3.2.2.1 National security certificates

38. According to section 79 DPA 2018, controllers may apply for national security certificates issued by a Minister, member of the Cabinet, the Attorney general or the Advocate General for Scotland, certifying that limitations of obligations and rights enshrined in Chapters 3 and 4 of Part 3 DPA 2018 are a necessary and proportionate measure for the protection of national security.
39. These certificates are meant to give controllers greater legal certainty, and will be conclusive evidence of the fact that national security is applicable when processing personal data. However, it should be mentioned that these certificates are not required in order to rely on national security restrictions but instead are a measure of transparency²⁶.
40. The EPDB understands from Schedule 20 DPA 2018, sections 17 and 18 that a national security certificate issued under the Data Protection Act 1998 (hereinafter “old certificate”) had an extended effect for the processing of personal data under the DPA 2018 until 25 May 2019. Until this date, unless replaced or revoked, the old certificates were treated as if they were issued under the DPA 2018. However, where there is no express expiry date on a national security certificate issued under the Data Protection Act 1998, the EDPB understands that such a certificate will continue to have effect in relation to processing under the Data Protection Act 1998, unless the certificate is revoked or quashed.²⁷ Even though the protection provided by these old certificates is limited to the processing of personal data under the Data Protection Act 1998, the EDPB takes note of the fact that new national security certificates can be issued under the Data Protection Act 1998 for personal data that was processed under the Data Protection Act 1998.²⁸
41. **For the sake of comprehensiveness, the EDPB invites the European Commission to clarify in its draft adequacy decision that national security certificates can still be issued under the Data Protection Act**

²⁶ See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018 - National_Security_Certificates_Guidance.pdf, p. 4.

²⁷ See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.

²⁸ See UK Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020, p. 5.

1998. Moreover, the EDPB invites the European Commission to describe in its draft adequacy decision the redress and oversight mechanisms with regard to certificates issued under the Data Protection Act 1998. Finally, the EDPB invites the European Commission to include in its draft adequacy decision the number of existing certificates issued under the Data Protection Act 1998, and to attentively monitor this aspect.

3.2.2.2 LED Automated decision-making

42. The EDPB stresses that Article 11(3) LED prohibits profiling that results in discrimination against natural persons on the basis of special categories of personal data. However, the EDPB notes that section 50 DPA 2018, which sets out the specific rules for automated decision making, foresees no such prohibition.
43. **The EDPB, therefore, invites the European Commission to verify this point, and explicitly state its findings in its adequacy decision. Moreover, the EDPB invites the European Commission to closely monitor cases related to automated decision making and profiling.**
44. According to the LED Adequacy Referential, "*[t]he third country law should, in any case, provide for necessary safeguards for the data subject's rights and freedoms. In this regard, the existence of a mechanism to inform the relevant Member State's competent authorities of any further processing such as the use of the transferred data for large scale profiling, should also be taken into account*"²⁹.
45. **The EDPB invites the Commission to assess this element in light of the guidance given by the EDPB in its referential.**

3.2.3 Onward transfers

46. According to the LED Adequacy Referential, onward transfers of personal data by the initial recipient to another third country or international organisation must not undermine the level of protection, provided for in the Union, of natural persons whose data is transferred. Therefore, such onward data transfers should be permitted only where the continuity of the level of protection afforded under EU law is ensured. The EDPB considers that, as pointed out by the European Commission in its assessment, the provisions under Chapter 5 of Part 3 DPA 2018, and in particular section 73, do in principle provide for a level of protection that is essentially equivalent to the one guaranteed under EU law, when it comes to transfer of personal data from a UK law enforcement authority to a third country.
47. First, section 73(1)(b) DPA 2018 notably provides that a controller may not transfer personal data to a third country or to an international organisation unless "*in a case where the personal data was originally transmitted or otherwise made available to the controller or another competent authority by a member State other than the United Kingdom, that member State, or any person based in that member State which is a competent authority for the purposes of the Law Enforcement Directive, has authorised the transfer in accordance with the law of the member State.*" Such provisions appear to be in line with the LED Adequacy Referential, which provides that the existence of a mechanism for the relevant Member State's competent authorities to be informed and authorise such onward transfer of data has also to be taken into account. The initial recipient of the data transferred from the EU should be liable and be able to prove that the relevant competent authority of the Member State has authorised the onward transfer, and that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision concerning the third country to which the data would be

²⁹ See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, paras 59-61.

onward transferred. “*In this context, the existence of an obligation or a commitment to implement relevant handling codes defined by the transferring Member States’ authorities should be taken into account*”³⁰.

48. **The EDPB invites the Commission to assess this element in light of the guidance given by the EDPB in its LED Adequacy Referential.**
49. Second, as explained in recital 81 of the draft decision, the UK Secretary of State has the power to recognise a third country (or a territory or a sector within a third country), an international organisation, or a description of such a country, territory, sector, or organisation as ensuring an adequate level of protection of personal data, following consultation of the ICO³¹. When assessing the adequacy of the level of protection, the UK Secretary of State must consider the same elements that the European Commission is required to assess under Article 36(2)(a)-(c) LED, interpreted together with recital 67 LED and the retained EU case-law. This means that, when assessing the adequate level of protection of a third country, the relevant standard will be whether that third country in question ensures a level of protection “essentially equivalent” to that guaranteed within the UK. Although the EDPB notes the capacity of the UK, under the DPA 2018, to recognise territories as providing an adequate level of protection in light of the UK data protection framework, the EDPB wishes to highlight that these latter territories might not benefit, to date, from an adequacy decision issued by the European Commission recognising a level of protection “essentially equivalent” to that guaranteed in the EU. This might lead to possible risks in the protection provided to personal data transferred from the EU, especially if the UK data protection framework were to deviate from the EU acquis in the future. It is to be noted that in July 2020, the *Schrems II* CJEU landmark case³² resulted in the invalidation of the US Privacy Shield Decision as, according to the CJEU, the US legal framework could not be considered as providing an essentially equivalent level of protection compared to the one of the EU. However, the already adopted judgments of the CJEU, considered as retained case-law in the UK legal framework, might not bind the UK anymore as, in particular, the UK has the possibility to modify retained EU law after the end of the bridge period, and its Supreme Court is not bound by any retained EU case-law³³.
50. **The EDPB therefore invites the European Commission to closely monitor the adequacy assessment process and criteria by UK authorities with regard to other third countries, in particular with respect to third countries not recognised as adequate under the LED by the EU.**
51. Where the European Commission would find that no essentially equivalent level of protection to that guaranteed within the EU, as per Article 36 LED, is ensured by the third country found adequate by the UK, **the EDPB invites the European Commission to take any and all necessary steps such as, for example, amending the UK adequacy decision to introduce specific safeguards for personal data originating from the EU, and/or to consider the suspension of the UK adequacy decision, where personal data transferred from the EU to the UK are subject to onward transfers to the third country in question on the basis of a UK adequacy regulation.**

³⁰ See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, paras 55 and 56.

³¹ See section 182(2) DPA 2018. See also the Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments, <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/>.

³² See CJEU, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems*, 16 July 2020, ECLI:EU:C:2020:559 (hereinafter “*Schrems II*”).

³³ See section 6(3) to (6) of the EU (Withdrawal) Act 2018.

52. Finally, in relation to the international agreements concluded, or to be concluded in the future, by the UK and the possible access, by authorities from third country(ies) party(ies) to such agreements, to personal data from the EU, the EDPB recommends that the European Commission examines the interplay between the UK data protection framework and its international commitments, in particular to ensure the continuity of the level of protection in case of onward transfers to other third countries of personal data transferred from the EU to the UK on the basis of a UK adequacy decision; and to continuously monitor and take action, where needed, with regard to the conclusion of international agreements between the UK and third countries that risk to undermine the level of protection of personal data provided for in the EU. For example, while the European Commission has referred to the fact that the UK-US CLOUD Act Agreement³⁴ may affect onward transfers to the US from service providers in the UK, the EDPB highlights that the entry into force of this agreement may also affect onward transfers from law enforcement authorities in the UK, in particular in relation to the issuance and transmission of orders as per Article 5 of the UK-US CLOUD Act Agreement.
53. The EDPB also considers that the conclusion of future agreements with third countries for the purpose of law enforcement cooperation, providing a legal basis for the transfer of personal data to these countries, may also significantly affect the conditions for onward sharing of the information collected, since such agreements may affect the UK data protection legal framework as assessed.
54. The EDPB therefore recommends that the European Commission continuously monitor whether the conclusion of future agreements between the UK and third countries may affect the application of UK data protection law, and provide for further limitation or exemption in relation to the onward sharing and the further use and disclosure overseas of information collected for law enforcement purposes. The EDPB considers that such information and assessment are essential in order to allow a comprehensive review of the level of protection afforded by the UK legislative framework and practices in relation to overseas disclosure.
55. Finally, the EDPB takes note that in accordance with section 76(4)(b) DPA 2018 (Transfers on the basis of special circumstances), law enforcement authorities in the UK may transfer personal data to a third country or an international organisation when the transfer “*is necessary for the purpose of obtaining legal advice in relation to any of the law enforcement purposes*”. The EPDB stresses that Article 38 LED does not contain a corresponding provision; therefore invites the European Commission to clarify what is meant by legal advice, and what kind of personal data is exchanged in such cases.

3.2.4 Further processing, including onward sharing for national security purposes

56. In its LED Adequacy Referential, the EDPB had pointed out that, concerning further processing or disclosure of data transferred from the EU for other purposes than law enforcement purposes, such as national security purposes, it should also be provided by law, be necessary and proportionate. As assessed by the European Commission in its draft decision, section 36(3) DPA 2018, the Digital Economy Act 2017, the Crime and Courts Act 2013, and the Serious Crime Act 2017 do provide for a clear legal framework allowing for onward sharing, providing that such onward sharing should be in compliance with the rules sets in the DPA 2018.
57. The EDPB notes that, in the context of further processing for other purposes of personal data transferred from the EU, the European Commission has not assessed whether there are any

³⁴ See Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Washington DC, USA, 3 October 2019, <https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019>.

mechanisms for the UK law enforcement authorities to inform the relevant Member States' competent authorities of a possible further processing of data. However, the LED Adequacy Referential considers this as an element which has to be taken into account³⁵. In addition, the existence of such mechanism to inform the relevant Member States' competent authorities of further processing of data for law enforcement purposes is also considered as an element to be taken into account under the LED Adequacy Referential³⁶.

58. **The EDPB thus invites the European Commission to complement its analysis with information about the existence of mechanisms for the UK law enforcement authorities to notify the relevant Member States' competent authorities of a possible further processing of data, transferred from the EU.**
59. Furthermore, with respect to the sharing of data collected by a criminal law enforcement authority with an intelligence agency for purposes of national security, the legal basis authorising such onward sharing is the Counter-terrorism Act 2008. In this regard, the EDPB notes that the scope and provisions of section 19 Counter-terrorism Act 2008 are not fully addressed in the European Commission's assessment, and may imply further use of a more broader nature, in particular as regards section 19(2) Counter-terrorism Act 2008, which provides that "*[i]information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.*" In this regard, the EDPB underlines that when further processed or disclosed, the data should benefit from the same level of protection as when they were processed initially by the receiving competent authority.

3.3 Oversight and enforcement

60. The EDPB notes that the oversight of criminal law enforcement agencies is ensured by a combination of different Commissioners, in addition to the ICO. The draft adequacy findings mentions the Investigatory Powers Commissioner (hereinafter "IPC"), the Commissioner for the Retention and Use of Biometric Material, as well as the Surveillance Camera Commissioner. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight. Of particular importance on questions of access to personal data transferred to the UK is the IPC. The understanding of the EDPB is that the IPC is a so-called "judicial commissioner", as other judicial commissioners, to be referred to in the context of national security chapter, and that those judicial commissioners enjoy the independence of judges, also when serving as commissioners. As to the office of the IPC, the European Commission explains in recital 245 of the draft decision that it functions independently as a so called "arm's length body", while being funded by the Home Office.
61. In addition, the IPC is also competent to the *ex-post* oversight of surveillance measures. It appears, however, that in this function the IPC's role is to make recommendations in cases of non-compliance, and to give notice to the data subject, if the error is serious and it is in the public interest for the person to be informed.
62. The EDPB has not found in the draft decision further indication to assess the independence of the Commissioner for the Retention and Use of Biometric Material, as well as of the Surveillance Camera Commissioner.
63. **The European Commission is invited to further assess the independence of the judicial commissioners, also in cases where the Commissioner is not (anymore) serving as a judge, as well as**

³⁵ See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 41 and footnote 39.

³⁶ See EDPB Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive, para 40.

to assess the independence of the Commissioner for the Retention and Use of Biometric Material, and as of the Surveillance Camera Commissioner.

Opinion of the Board (Art. 64)



Opinion 19/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 1 June 2021

Table of contents

1	Summary of the Facts	4
2	Assessment	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX	6
2.2.2	GENERAL REMARKS	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION	7
2.2.4	RESOURCE REQUIREMENTS.....	7
2.2.5	PROCESS REQUIREMENTS.....	8
3	Conclusions / Recommendations	8
4	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Hungarian Supervisory Authority (hereinafter “HU SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 06 April 2021. The HU national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the HU SA, once they are approved by the HU SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the HU SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.
3. This assessment of HU SA’s additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB’s

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the HU SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the HU SA to take further action.
8. This opinion does not reflect upon items submitted by the HU SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
 - b. independence of the certification body
 - c. conflicts of interests of the certification body
 - d. expertise of the certification body
 - e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
 - f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
 - g. transparent handling of complaints about infringements of the certification.
9. Taking into account that:

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
- e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
- f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

[2.2.1 PREFIX](#)

10. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

[2.2.2 GENERAL REMARKS](#)

11. The Board notes that the requirements should be drafted in a prescriptive manner. Thus, the requirements should avoid the word “should” and rather use “shall” or “must”. The EDPB encourages the HU SA to make the necessary changes in this regard (e.g. in section 7.4, 2nd, 5th and 6th paragraphs; section 7.6, 1st paragraph; section 7.7, 3rd paragraph; section 7.11, 1st paragraph; sections 7.12, 7.13 and 9.3.3)
12. In addition, the Board encourages the HU SA to use consistent wording and ensure that the requirements are drafted in a way that ensure clarity. In this regard, the Board notes that, for example, paragraph 3 of section 4.1.2 could refer to the powers of the NAIH “which is competent” in line with the GDPR, section 7.1.1 could refer to the additional requirements “of the NAIH”; section 4.2 should refer to “Regulation” 765/2008/EC. In addition, for the sake of clarity, the references to “the competent SA” should be replaced by “HU SA” or “the NAIH” in section 9.3.3.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

13. With regard to section 4.1.1 of the HU SA's draft accreditation requirements, and in particular, the last sentence of the second paragraph, the Board considers that the reference to the subject matter of the ToE is not entirely correct in this case, since the requirement is related to the accreditation of the certification bodies and not to their certification activities. Therefore, the Board encourages the HU SA to delete the said reference in the last part of the requirement.
14. Regarding section 4.1.2, point 7, the EDPB notes that the HU SA's draft accreditation requirements establish that the certification agreement shall allow the certification body to "disclose all information necessary to the EDPB and NAIH for granting certification". Whereas the EDPB welcome the explicit reference to the HU SA, which provides clarity, the reference to the EDPB seems less accurate, given that article 42(8) GDPR does not specify the manner in which the EDPB will collate the information. Thus, the EDPB considers that the wording of the Annex, which provide for more flexibility, is more appropriate and encourages the HU SA to redraft the requirements in this line.
15. With regard to section 4.2 ("Management of impartiality"), the Board encourages the HU SA to provide examples of situations where a certification body has no relevant connection with the customer it assesses. For example, the certification body should not belong to the same company group nor should be controlled in any way by the customer it assesses.

2.2.4 RESOURCE REQUIREMENTS

16. Concerning certification body personnel (section 6.1), the Board notes that the requirements follow the Annex. In this respect, the Board is of the Opinion that, with regard to the expertise of the certification body, the emphasis should be put on the different type of substantive expertise and experience. Specifically, the Board considers that the competence requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In the Board's opinion, evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. On this respect, the Board considers that the requirements for personnel with technical expertise and for personnel with legal expertise should be more aligned, so as to avoid the situation in which personnel with technical expertise have significantly less expertise than personnel with legal expertise. Instead, the focus should be made on the differences between evaluators and decision-makers in terms of their expertise and experience. Considering this, the Board encourages the HU SA to redraft this section taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.
17. With regard to the legal personnel in charge of certification decisions, the Board notes that the HU SA's draft accreditation requirements determine a minimum of five years of professional experience in data protection law. In this regard, the Annex refers to "significant" professional experience, which encompasses not only quantitative elements but also qualitative ones. Thus, in order to ensure clarity, the Board encourages the HU SA to clarify that the required years of professional experience have to be relevant for the tasks they will perform.

2.2.5 PROCESS REQUIREMENTS

18. Section 7.1 par. 2 of the HU SA's draft accreditation requirements establishes the obligation to notify the HU SA before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office. The EDPB notes that this obligation is towards all the competent supervisory authorities and recommends the HU SA to amend the draft accordingly.
19. Furthermore, the Board notes that the use of external experts contracted by the certification body is foreseen in the HU SA's draft accreditation requirements. The Board considers that the draft accreditation requirements should explicitly state that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the HU SA to amend the draft accordingly.
20. The Board notes that the second paragraph of section 7.6 of the HU SA's draft accreditation requirements ("certification decision") includes the obligation to submit the draft approval to the HU SA, prior to issuing or renewing certification. Based on the explanations provided by the HU SA, the Board understand that the intention of this requirement is to increase transparency and, in case that the HU SA decides, on the basis of the information, to start an investigation, it will not suspend the certification process. The Board encourages the HU SA to include a clarification in that sense.
21. With regard to last paragraph of section 7.6 ("Certification decision"), the Board encourages to clarify that the investigations or procedure referred which may prevent certification being issued are those related to the target of evaluation or the scope of the certification.
22. Finally, with regard to section 7.9 ("Surveillance"), the EDPB notes that the draft requirements do not establish a specific period for the monitoring. In this regard, the Board considers that, when determining the periodicity of the surveillance, the risk associated with the processing should be taken into account. Even in those cases where a specific frequency for the monitoring is determined, a risk-based approach is necessary to assess whether a more frequent monitoring is needed. Thus, the EDPB encourages the HU SA to introduce a risk-based approach in order to determine the frequency of the surveillance. This does not prevent the HU SA to also include minimum deadlines for monitoring, combined with a risk-based approach.

3 CONCLUSIONS / RECOMMENDATIONS

23. The draft accreditation requirements of the Hungarian Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
24. Regarding 'process requirements', the Board recommends that the HU SA:
 - 1) amend section 7.1, par. 2 in order to refer to all the competent supervisory authorities.
 - 2) explicitly state that the certification body will retain the responsibility for the decision-making, even when it uses external experts

4 FINAL REMARKS

25. This opinion is addressed to the Hungarian Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
26. According to Article 64 (7) and (8) GDPR, the HU SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
27. The HU SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 8/2020 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Reinsurance Group of America

Adopted on 14 April 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (EEA) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the EDPB) is to ensure the consistent application of the GDPR throughout the European Economic Area. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (SA) aims to approve binding corporate rules (BCRs) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under the Directive 95/46/EC the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR and, in addition, conferred to the EDPB the task to issue an opinion on the competent supervisory authority’s (BCR Lead) draft decision aiming to approve BCRs. This task of EDPB aims to ensure the consistent application of the GDPR, including by the supervisory authorities, controllers and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent supervisory authority (“competent SA”), in accordance with the consistency mechanism set out in Article 63 and 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party¹, endorsed by the EDPB.

¹ The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) WP256 rev.01 of the Article 29 Working Party,² as endorsed by the EDPB, provides for the required elements for BCRs for controllers, including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance to the supervisory authorities' national laws. The EDPB is subject to Regulation 1049/2001 pursuant to article 76(2) GDPR.

(5) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2), each application should be addressed individually and is without prejudice to the assessment of any other Binding Corporate Rules. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake and the policies and procedures that they have in place to protect personal data.³

(6) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft Controller BCRs of Reinsurance Group of America were reviewed by the Irish Data Protection Commission (hereinafter Irish Supervisory Authority) as the BCRs Lead SA.
2. The Irish Supervisory Authority has submitted its draft decision regarding the draft Controller BCRs of Reinsurance Group of America, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 18/02/2020. The decision on the completeness of the file was taken on 26/03/2020.

2 ASSESSMENT

3. The EDPB notes that the Reinsurance Group of America has only provided one Intra Group Agreement (IGA), common to both the Controller BCR and Processor BCR. Since Reinsurance Group of America has provided two different sets of BCRs and Annexes, and the IGA makes a clear distinction in its relevant provisions, the EDPB considers that no further documents need to be submitted in this regard.

² Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

³ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

4. The Reinsurance Group of America draft Controller BCRs apply to processing carried out by RGA or any of its subsidiaries, either as a controller or as a processor acting on behalf of another group member, of personal data processed within and transferred outside of the EEA.
5. Concerned data subjects include current and past employees, temporary members of the workforce engaged by any group member, job applicants, individual consultants and independent contractors, representatives of customers and other business partners, individuals who are parties to or beneficiaries of primary individual or group insurance and pension policies, individual contractors and account managers and staff of third party suppliers who provide services to RGA, as well as third parties with whom RGA engages for legitimate business-related purposes.
6. The Reinsurance Group of America draft Controller BCRs have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Reinsurance Group of America draft Controller BCRs contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the Irish Supervisory Authority submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns, which need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

7. Taking into account the above and the commitments that the group members will undertake by signing Reinsurance Group of America's Intra-Group Agreement on Binding Corporate Rules, the EDPB considers that the draft decision of the Irish Supervisory Authority may be adopted as it is, since those Rules ensure appropriate safeguards to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the Irish Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the Irish Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the Irish Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



Opinion 12/2020 on the draft decision of the competent supervisory authority of Finland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 25 May 2020

Table of contents

1	SUMMARY OF THE FACTS	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the FI accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	6
2.2.3	CONFLICT OF INTEREST	7
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES	8
2.2.5	TRANSPARENT COMPLAINT HANDLING.....	9
2.2.6	LEGAL STATUS	9
3	CONCLUSIONS / RECOMMENDATIONS.....	9
4	FINAL REMARKS	10

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Finnish Supervisory Authority (hereinafter "FI SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 17 February 2020.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the FI SA to take further action.
8. This opinion does not reflect upon items submitted by the FI SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the FI accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The Board observes that, according to the general notes of the draft accreditation requirements, the FI SA will review the accreditation of the monitoring body “periodically” according to risk-based approach to ensure that the body still meets the requirements for accreditation. The Board welcomes the provision concerning the periodic re-assessment of the accreditation requirements by the FI SA in order to ensure compliance with the GDPR. However, for the sake of clarity and transparency, the Board encourages the FI SA to provide information on how periodic review will work in practice.
11. With regards to the expertise requirements, section 3.1 of the FI SA’s draft accreditation requirements states that the monitoring body shall be compliant with data protection legislation in its own actions. Indeed, it is unclear how the data protection legislation compliance will be checked by the FI SA, for

example, whether a self-declaration of the monitoring body in this regard would be enough or a more comprehensive assessment will be carried out by the SA. Therefore, the Board recommends that the FI SA redraft this requirement in terms of accountability, clarifying that the monitoring body shall demonstrate compliance with data protection legislation.

12. The Board encourages the FI SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.

2.2.2 INDEPENDENCE

13. The Board notes that, according to the general notes of the draft accreditation requirements, the requirements shall apply to a monitoring body regardless of whether it is an internal or an external body, unless stated otherwise. The Board is of the opinion that internal monitoring bodies cannot be set up within a code member, but only within a code owner. Therefore, the Board recommends that this is clarified and reflected either in the text of the draft accreditation requirements or as an example.
14. With regard to the first paragraph of the explanatory note under the section 1 of the FI SA's draft accreditation requirements ("Independence"), the Board acknowledges the impartiality of the monitoring body from the code members, the profession, industry or sector to which the code applies. However, the Board is of the opinion that these requirements should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members. For this reason, the Board encourages the FI SA to amend this paragraph accordingly.
15. With regard to the second paragraph of the explanatory note under the "Independence" section of the FI SA's draft accreditation requirements, the Board notes the structural and procedural requirements to ensure independence. The Board recommends that the FI SA redraft the requirements in order to emphasize the fact that it is the monitoring body requesting accreditation that should prove its independence.
16. Furthermore, the Board notes that the monitoring body shall have the financial stability and resources for the operation of its activities and obtain financial support for its monitoring role in a way that does not compromise its independence (section 1.1. and 1.3 of the FI SA's draft accreditation requirements). However, the Board considers that further explanation is needed as to how long-term financial stability of the monitoring body is ensured. In particular, the Board recommends that the FI SA redraft the requirements in order to explain how financial independence is guaranteed in case one or more funding sources are no longer available. Furthermore, the Board considers that section 1.4 of the FI SA's draft accreditation requirements should also include a reference to the need of ensuring clarifications as to how financial independency is ensured with regard to the risks associated with the monitoring body's own activities, for example in case of damages that need to be paid due to the monitoring body's liability. The Board therefore recommends that the FI SA include such reference in the draft accreditation requirements. Finally, the Board considers that section 1.4 of the FI SA's draft accreditation requirements would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support would not adversely affect its independence. For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the

monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the FI SA to provide examples of how the monitoring body can provide such evidence.

17. With regard to the appointment of members/personnel of the monitoring body (section 1.5 of the FI SA's draft accreditation requirements), the Board recommends that the FI SA clarify how the independence of the monitoring body could be demonstrated, aligning the wording of the requirement to this of the Guidelines (see paragraphs 63 to 67), for clarification purposes.
18. Section 1.12 of the FI SA's draft accreditation requirements refers to the organisational structure of the internal monitoring body and ensures its impartiality, by requesting that it has separate members/personnel and management. The Board acknowledges that this wording is based on the Guidelines. Nonetheless, the Board is of the opinion that a strict obligation of using personnel outside the internal monitoring body could be difficult to achieve in certain situations. For this reason, the Board encourages the FI SA to soften the requirement, in order to allow those exceptional situations in which it would not be possible for an internal monitoring body to have separate members/personnel and management from the larger entity it belongs to, as long as there are appropriate safeguards in place to sufficiently mitigate a risk of independence or a conflict of interest (paragraph 66, page 22 of the Guidelines).
19. Section 1.13 of the FI SA's draft accreditation requirements refers to the use of sub-contractors by the monitoring body. The Board is of the opinion that the sub-contractors should be able to ensure the same degree of safeguards provided by the monitoring body in performing their activities, including the same level of competence and expertise. At the same time, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the FI SA to specify that, notwithstanding the sub-contractor's responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance. In addition, the Board is of the opinion that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. The Board recommends the FI SA to explicitly add this obligation in the draft accreditation requirements.
20. The Board observes that, according to section 1.15 of the FI SA's draft accreditation requirements, when using sub-contractors for processes relating to monitoring actions, the monitoring body shall deliver written contracts or agreements to outline responsibilities etc., as well as documentation of the procedure for subcontracting. The Board encourages the FI SA to redraft the text in order to include requirements relating to the termination of those contracts, in particular so as to ensure that the subcontractors fulfil their data protection obligations. Additionally the Board encourages the FI SA to add requirements relating to the risk management of the appointment of the external body.

2.2.3 CONFLICT OF INTEREST

21. The Board takes note of the requirements included in the FI SA's draft accreditation requirements, in order for the monitoring body to demonstrate that the exercise of its tasks and duties does not result in a conflict of interest. However, the explanatory note under section 2 of the draft requirements does not provide enough clarity as to which situations may result in conflict of interest. The Board is of the opinion that, for practical reasons, examples of cases where conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting

audits or making decisions on behalf of a monitoring body had previously worked in the recent years for the code owner, or for any of the organisations adhering to the code in the recent years. Therefore, the Board encourages the FI SA to add some examples, similar to the one provided in this paragraph. Furthermore, the Board encourages the FI SA to redraft the requirement under this section, so that it is clarified that conflicts of interest might also depend on the specificities of the sector(s) to which the CoC applies.

22. The Board acknowledges that the explanatory note under section 2 of the FI SA's draft accreditation requirements refers to the identification of situations likely to create conflict of interest and the fact that measures will be taken in order to avoid such conflict. However, the Board is of the opinion that, with regard to internal monitoring bodies, the requirements relating to the burden of proof of the absence of conflict of interest should be stricter and recommends that the requirements be redrafted accordingly.
23. Section 2.1 of the FI SA's draft accreditation requirements states that the monitoring body shall not provide any services to code members that would adversely affect its impartiality. The Board welcomes this requirement, however it considers that risks to impartiality may arise from a wide range of activities carried out by the monitoring body also vis-à-vis code owners (especially if the monitoring body is internal) or other relevant bodies of the sector concerned. Therefore, the Board encourages the FI SA to supplement the current requirement accordingly.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

24. With regard to established procedures and structures, the Board observes that the requirements under section 4 of the FI SA's draft accreditation requirements are presented in a general manner. The Board is of the opinion that the procedures to monitor compliance with codes of conduct have to be specific enough to ensure a consistent application of the obligations of code monitoring bodies.
25. In particular, such procedures need to address the complete monitoring process, from the preparation of the evaluation to the conclusion of the audit and additional controls to ensure that appropriate actions are taken to remedy infringements and to prevent repeated offences. In addition, the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear timeframe, and check the eligibility of members prior to joining the code.² Therefore, the Board recommends that the FI SA develop further these requirements and add examples of the above procedures (such as, procedures providing for audit plans to be carried out over a definite period and on the basis of predetermined criteria, a specific control methodology and the documentation and assessment of the findings as well as the full cooperation by the code members).
26. Section 4.4 of FI SA's the draft accreditation requirements makes reference to descriptions of corrective measures in case of infringement that need to be delivered to the FI SA. The Board is of the opinion that those corrective measures must be determined in the code of conduct, as per article 40(4) GDPR. Therefore, the Board recommends the FI SA to make reference to the list of measures set out

² The EDPB provided some examples of such procedures in section 2.2.4 of the Opinion 9/2019 on the Austrian SA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR.

in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.

2.2.5 TRANSPARENT COMPLAINT HANDLING

27. Regarding section 5.1 of the FI SA's draft accreditation requirements, the Board acknowledges that the monitoring body should establish effective procedures and structures to handle complaints in an impartial and transparent manner. In this regard, the Board notes that the FI SA's draft accreditation requirements include a description of the procedure for complaints handling. However, the Board is of the opinion that further clarification is needed with regard to the "estimated timeframe" for answering complaints. In this regard, the procedure shall envisage that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame. This period could be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation. Therefore, the Board recommends that the requirement is redrafted accordingly.
28. Regarding section 5.4 of the FI SA's draft accreditation requirements, the Boards notes that the monitoring body's decisions, or general information thereof, shall be made publicly available in line with its complaints handling procedure. Without prejudice to national legislation, the Board encourages the FI SA to amend this requirement so that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate. However, data subjects should, in any case, be informed about the status and outcome of their individual complaints, so that the transparency requirements of this procedure are respected.

2.2.6 LEGAL STATUS

With regard to the legal status of the monitoring body, section 8.2 of the FI SA's draft accreditation requirements states that the monitoring body shall have adequate resources for specific duties and responsibilities over a suitable period of time. The Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the monitoring mechanism over time. Thereby, the Board encourages the FI SA to redraft the requirement accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

29. The draft accreditation requirements of the Finish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
30. Regarding *general remarks* the Board recommends that the FI SA:
 1. redraft section 3.1 in terms of accountability, clarifying that the monitoring body shall demonstrate compliance with data protection legislation.
31. Regarding *independence* the Board recommends that the FI SA:
 1. clarify, either in the text of the requirements or as an example, that internal monitoring bodies cannot be set up within a code member, but only within a code owner.

2. redraft the second paragraph of the explanatory note, so that it is emphasised that it is the monitoring body requesting accreditation the one that should prove its independence.

3. redraft sections 1.1. and 1.6 to explain how financial independence is guaranteed when one or more funding sources are no longer available.

4. include in section 1.4 clarifications as to how financial independence is ensured with regard to the risks associated with the monitoring body's own activities, for example in case of damages that need be paid due to the monitoring body's liability.

5. clarify how the independence of the monitoring body could be demonstrated by aligning the wording of the requirement to this of the Guidelines, with regard to the appointment of members/staff of the monitoring body in section 1.5.

6. add in section 1.13 that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.

32. Regarding *conflict of interest* the Board recommends that the FI SA:

1. redraft the requirements under the explanatory note in section 2 relating to the internal monitoring bodies in a stricter way, in order to include the burden of proof of the absence of conflict of interest.

33. Regarding *established procedures and structures* the Board recommends that the FI SA:

1. further develop under section 4 the procedures to monitor compliance with codes of conduct and includes examples of such procedures.

2. refer in section 4.4 to the list of corrective measures set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.

34. Regarding *transparent complaint handling* the Board recommends that the FI SA:

1. redraft section 5.1 to indicate that the procedure for answering complaints shall envisage the obligation for the monitoring body to inform the complainant with progress reports or the outcome of the complaint within a reasonable time frame. Such timeframe can be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation.

4 FINAL REMARKS

35. This opinion is addressed to the Finnish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.

36. According to Article 64 (7) and (8) GDPR, the FI SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

37. The FI SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 24/2020 on the draft decision of the Norwegian Supervisory Authority regarding the Controller Binding Corporate Rules of Jotun

Adopted on 31 July 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.
- (2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.
- (3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Jotun were reviewed by the Norwegian Supervisory Authority (Datatilsynet) as the Competent SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Jotun, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 15 May 2020. The decision on the completeness of the file was taken on 9 June 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01 - endorsed by the EDPB.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264 - endorsed by the EDPB.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Jotun covers all processing of personal data carried out by Jotun A/S and its Group Companies, either acting as a controller or as a processor on-behalf of another Group Company, and all transfers of personal data within the Jotun Group Companies.
4. Concerned data subjects include Employees, Customers and their employees, as well as Suppliers and their employees⁷.
5. The draft BCR-C of Jotun has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of Jotun contains all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Jotun contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁸, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, Jotun A/S and its Group Companies should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁷ As those terms are defined in the ‘Definitions’ section of Jotun’s BCR-C.

⁸ CJEU, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 25/2020 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Tetra Pak

Adopted on 31 July 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.
- (2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.
- (3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Tetra Pak were reviewed by the Swedish Supervisory Authority (Datainspektionen) as the Competent SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Tetra Pak, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 5 June 2020. The decision on the completeness of the file was taken on 18 June 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01 - endorsed by the EDPB.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Tetra Pak covers all processing of personal data carried out by the Tetra Pak BCR Members.⁶
4. Concerned data subjects include employees, emergency contacts and family members of the employees, contingent workforce, job applicants and candidates, customers, suppliers and other third parties occupied by the employees or contingent workforce in the course of regular business dealings.
5. The draft BCR-C of Tetra Pak has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCRs-C of Tetra Pak contains all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Tetra Pak Intra-Group BCR Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs-C of Tetra Pak contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, Tetra Pak and its Group Companies should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁶ As the “Tetra Pak BCR Members” defined in the ‘Definitions’ section of Tetra Pak’s BCR-C.

⁷ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



Opinion 9/2023 on the draft decision of the Italian Supervisory Authority regarding the Controller Binding Corporate Rules of Vertiv

Adopted on 17 May 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Vertiv S.r.l and the group's entities (hereinafter "**Vertiv Group**") was reviewed by the Italian SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of Vertiv Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 17 March 2023. The decision on the completeness of the file was taken on 30 March 2023.

2 ASSESSMENT

3. The draft BCR-C of Vertiv Group covers the processing of personal data by Vertiv Group members legally bound by the BCRs and they apply to the intra-group transfers of personal data to third countries by members of the Vertiv group acting as controllers⁷.
4. Concerned data subjects include Vertiv group's employees, clients (including potential clients), candidates, website users, related parties, related parties' family members and suppliers⁸.
5. The draft BCR-C of Vertiv Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Vertiv Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement annexed to the BCR-C, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of Vertiv Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

⁷ Vertiv BCR-C, Section 3.

⁸ Vertiv BCR-C, Section 3.1

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 10/2023 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the PROSEGUR Group

Adopted on 30 June 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “the BCR Lead”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the PROSEGUR Group was reviewed by the Spanish Supervisory Authority as the BCR Lead SA.
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of the PROSEGUR Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 19th April 2023. The decision on the completeness of the file was taken on 12 May 2023.

2 ASSESSMENT

3. The draft BCR-C of PROSEGUR Group covers international transfers of personal data between PROSEGUR Group members legally bound by the BCRs, as well as to any subsequent international transfer and processing of personal data within the Group, when PROSEGUR Group members act as controllers or as processors on behalf of another controller of the Group⁷.
4. Concerned data subjects are: job candidates; suppliers, users, potential and current customers including their representatives or contact persons; employees and their beneficiaries or relatives (including minors); tenants and landlords⁸.
5. The draft BCR-C of the PROSEGUR Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the PROSEGUR Group contains all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intragroup Agreement regarding Binding Corporate Rules, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of the PROSEGUR Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries

⁷ See Section 3.1 of the BCR-C.

⁸ See Section 3.2.2 BCR-C and Annex 2.

included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 16/2023 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Informatica Group

Adopted on 28 September 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS.....	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Informatica Ireland EMEA UC and the group's entities (hereinafter the "**Informatica Group**") was reviewed by the Irish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Informatica Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 20 July 2023. The decision on the completeness of the file was taken on 8 August 2023.

2 ASSESSMENT

3. The draft BCR-C of the Informatica Group covers the processing of personal data by Informatica Group entities as well as intra-group transfers of personal data to third countries among the Informatica Group entities⁹, legally bound by the BCR.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Informatica BCR-C, p.3, III B., "Geographical Scope"

4. Concerned data subjects include prospective, current and future employees (and their declared relatives), HR agents and operators, vendors, business partners, advisors, customers and prospective customers business contacts processed by the Informatica Group¹⁰.
5. The draft BCR-C of the Informatica Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Informatica Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement¹¹, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Informatica Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

¹⁰ Informatica BCR-C, p.3, III C., “Substantive Scope” and p.24-27 Appendix F, “Business Contact Data and Employee Data”.

¹¹ Referred as “Interaffiliate Data Processing and Transfer Agreement” in the application form.

Opinion of the Board (Art. 64)



Opinion 17/2023 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Informatica Group

Adopted on 28 September 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Informatica Ireland EMEA UC and the group's entities (hereinafter the "**Informatica Group**") was reviewed by the Irish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Informatica Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on [date]. The decision on the completeness of the file was taken on 8 August 2023.

2 ASSESSMENT

3. The draft BCR-P of the Informatica Group covers all intra-Group transfers and processing of personal data by Informatica Group entities legally bound by the BCR-P, when they act as processors on behalf of controllers outside of the Group⁷.
4. Concerned data subjects include Informatica Group's customers, their customers and users and other data subjects whose data is processed on behalf of the controller pursuant to a contract or other legal act⁸.
5. The draft BCR-P of the Informatica Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Informatica Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement⁹, the EDPB considers that the draft decision of the BCR Lead may be

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Informatica Group BCR-P, Part III.

⁸ Informatica Group BCR-P, Part III.C.

⁹ Referred as "Agreement to be bound by Informatica BCRs in respect of Regulation (EU) 2016/679" in the application form.

adopted as it is, since the draft BCR-P of the Informatica Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 36/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the Booking.com Group

Adopted on 28 December 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Booking.com Holding B.V. and its entities (hereinafter the "**Booking.com Group**") was reviewed by the NL SA as the BCR Lead.
2. The NL SA has submitted its draft decision regarding the draft BCR-C of the Booking.com Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 16 November 2023. The decision on the completeness of the file was taken on 29 November 2023.

2 ASSESSMENT

3. The draft BCR-C of the Booking.com Group covers transfers of personal data from the EEA to countries outside the EEA amongst Booking.com Group Members, legally bound by the BCR-C, and their employees worldwide which process personal data as a controller⁹.
4. Concerned data subjects include customers, accommodation partners, affiliate partners and other contractors, and employee data¹⁰.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Booking.com Controller Binding Corporate Rules Policy p.1 (introduction to this BCR policy) and section 1.4 "What is booking.com doing about it?". For more details see Booking.com Group Members Overview.

¹⁰ Booking.com Controller Binding Corporate Rules Policy, p. 1 (introduction to this BCR policy).

5. The draft BCR-C of the Booking.com Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Booking.com Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Intra-group Agreement regarding the Binding Corporate Rules of Booking.com*, the EDPB considers that the draft decision of the NL SA may be adopted as it is, since the draft BCR-C of the Booking.com Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the NL SA and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 7/2023 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of Autodesk Group

Adopted on 5 May 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data i nstituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR C of Autodesk Ireland Operations Unlimited and the group's entities (hereinafter "**Autodesk Group**") was reviewed by the Irish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of Autodesk Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 10 March 2023. The decision on the completeness of the file was taken on 30 March 2023.

2 ASSESSMENT

3. The draft BCR-C of Autodesk Group covers the processing of personal data by Autodesk Group members legally bound by the BCRs, when they act as controllers or as processors on behalf of another controller of the Group⁷ and they apply to all transfers of personal data within the Group⁸.
4. Concerned data subjects include Autodesk group's customers, workers and suppliers⁹.
5. The draft BCR-C of Autodesk Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Autodesk Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement for Controller Binding Corporate Rules (BCR-C) and Processors Binding Corporate Rules (BCR-P), the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of Autodesk Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as

⁷ Autodesk Group BCR-C, Part 1, Section 5, Appendix 1

⁸ Autodesk Group BCR-C, Part 1, Section 5, Appendix 1

⁹ Autodesk Group BCR-C, Part 1, Section 5, Appendix 1

the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 8/2023 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Autodesk Group

Adopted on 5 May 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Autodesk Ireland Operations Unlimited and the group's entities (hereinafter "**Autodesk Group**") was reviewed by the Irish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Autodesk Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 30 March 2023. The decision on the completeness of the file was taken on 10 March 2023.

2 ASSESSMENT

3. The draft BCR-P of the Autodesk Group covers the processing of personal data by Autodesk Group members legally bound by the BCRs, when they act as processors on behalf of non Autodesk controllers established in the EU⁷ and they will geographically apply as determined by the relevant controller⁸.
4. Concerned data subjects include Autodesk group's end users⁹.
5. The draft BCR-P of Autodesk Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Autodesk Group contains all elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement for Controller Binding Corporate Rules (BCR-C) and Processors Binding Corporate Rules (BCR-P), the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of Autodesk Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Autodesk Group BCR-P, Part 1, Section 5.

⁸ Autodesk Group BCR-P, Part 1, Section 5.

⁹ Autodesk Group BCR-P, Part 1, Section 5.

is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 70.1.s)



**Opinion 32/2021 regarding the European Commission Draft
Implementing Decision pursuant to Regulation (EU)
2016/679 on the adequate protection of personal data in
the Republic of Korea**

Version 1.0

Adopted on 24 September 2021

CONTENTS

1.	EXECUTIVE SUMMARY	4
1.1.	Areas of convergence	4
1.2.	Challenges.....	5
1.2.1.	General	5
1.2.2.	General data protection aspects	6
1.2.3.	On the access by public authorities to data transferred to the Republic of Korea ..	7
1.3.	Conclusion	8
2.	INTRODUCTION.....	8
2.1.	Korean data protection framework.....	8
2.2.	Scope of the EDPB's assessment.....	9
2.3.	General comments and concerns	10
2.3.1.	International commitments entered into by the Republic of Korea	10
2.3.2	Scope of the adequacy decision	10
3.	GENERAL DATA PROTECTION ASPECTS	11
3.1.	Content principles	11
3.1.1.	Concepts	12
3.1.2.	Partial exemptions provided for in PIPA	13
3.1.3	Grounds for lawful and fair processing for legitimate purposes	15
3.1.4	The purpose limitation principle	16
3.1.5	The data quality and proportionality principle	16
3.1.6	Data retention principle	17
3.1.7	The security and confidentiality principle	17
3.1.8	The transparency principle	18
3.1.9	Special categories of personal data	19
3.1.10	Rights of access, rectification, erasure and objection	19
3.1.11	Restrictions on onward transfers	22
3.1.12	Direct marketing	23
3.1.13	Automated decision-making and profiling	24
3.1.14	Accountability	25
3.2.	Procedural and Enforcement Mechanisms	25
3.2.1	Competent Independent Supervisory Authority.....	25
3.2.2.	Existence of a data protection system ensuring a good level of compliance	26

3.2.3. The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms	27
4. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN SOUTH KOREA	27
4.1 General data protection framework in the context of government access	28
4.2 Protection and safeguards for communication confirmation data in the context of government access for law enforcement purposes	28
4.3 Access to communication information by Korean public authorities for national security purposes.....	30
4.3.1 No obligation to notify individuals of government access to communications between foreign nationals	30
4.3.2 No prior independent authorisation for collection of communication information between foreign nationals	31
4.4 Voluntary disclosures.....	32
4.5 Further use of information	33
4.6 Onward transfers and intelligence sharing	33
4.6.1 Applicable legal framework for onward transfers by law enforcement authorities	34
4.6.2 Applicable legal framework for onward transfers for national security purposes ...	35
4.6.3 International agreements	36
4.7 Oversight	36
4.8 Judicial remedy and redress	37

The European Data Protection Board

Having regard to Article 70(1)(s) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (“**GDPR**”),

Having regard to the European Economic Area (“**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION:

1. EXECUTIVE SUMMARY

1. The European Commission launched the formal process towards the adoption of its draft implementing decision (“**draft decision**”) on the adequate protection of personal data in the Republic of Korea under the Personal Information Protection Act pursuant to the GDPR on 16 June 2021².
2. On the same date, the European Commission asked for the opinion of the European Data Protection Board (“**EDPB**”)³. The EDPB’s assessment of the adequacy of the level of protection afforded in the Republic of Korea has been made on the basis of the examination of the draft decision itself as well as on the basis of an analysis of the documentation made available⁴ by the European Commission.
3. The EDPB focused on the assessment of both, the general GDPR aspects of the draft decision and the access by public authorities to personal data transferred from the EEA for the purposes of law enforcement and national security, including the legal remedies available to individuals in the EEA. The EDPB also assessed whether the safeguards provided under the Korean legal framework are in place and effective.
4. The EDPB has used as main reference for this work its GDPR Adequacy Referential⁵ (“**GDPR Adequacy Referential**”) adopted in February 2018 and the EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures⁶.

1.1. Areas of convergence

5. The EDPB’s key objective is to give an opinion to the European Commission on the adequacy of the level of protection afforded to individuals whose personal data is transferred to the Republic of Korea.

¹ References to “**Member States**” made throughout this opinion should be understood as references to “EEA Member States”.

² See press release https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.

³ Ibid.

⁴ The EDPB based its analysis on official translations prepared by the Korean government.

⁵ WP254, GDPR Adequacy Referential, 6 February 2018, (endorsed by the EDPB, see <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>).

⁶ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

It is important to recognise that the EDPB does not expect the Korean data protection framework to replicate European data protection law.

6. However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 45 GDPR and the case-law of the Court of Justice of the European Union (hereinafter “**CJEU**”) require the third country’s legislation to be aligned with the essence of the fundamental principles enshrined in the GDPR. In this context, the Korean data protection framework presents numerous similarities to the European data protection framework, having one main piece of legislation covering both, the public and the private sector, and which is completed by sector-specific legislative acts.
7. With regards to the content, the EDPB notes key areas of alignment between the GDPR framework and the Korean data protection framework with regard to certain core provisions such as, for example, concepts (e.g., “personal information”, “processing”, “data subject”); grounds for lawful and fair processing for legitimate purposes; purpose limitation; data quality and proportionality; data retention, security and confidentiality; transparency; and special categories of data.
8. In addition to the above, the EDPB welcomes the efforts made by the European Commission and the Korean authorities to ensure that the Republic of Korea provides an adequate level of protection to that of the GDPR through the adoption of Notifications by the Korean supervisory authority (applicable not only to personal data transferred from the EEA to Korea) with the aim to fill in the gaps between the GDPR and the Korean data protection framework. In this context, the EDPB wishes to highlight the relevance of these Notifications for the assessment of the adequacy of the Republic of Korea noting, for example, that they provide relevant clarifications on some important safeguards, *inter alia* in relation to the scope of application of the exemptions from the PIPA for the processing of pseudonymised personal information for scientific, research and statistical purposes, onward transfers and the rules applicable in the context of access to data by public authorities.

1.2. Challenges

9. While the EDPB has identified many aspects of the Korean data protection framework to be essentially equivalent to the European data protection framework, it has also concluded that there are certain aspects that may require a closer look and clarification. Specifically, the EDPB considers that the following items should be further assessed to ensure that the essentially equivalent level of protection is met, and that they should be closely monitored by the European Commission.

1.2.1. General

10. The EDPB takes note that the Notification No 2021-1 *has the status of an administrative rule with legally binding force on the personal information controller in the sense that any violation of th[e] Notification may be regarded as a violation of the relevant provisions of PIPA*⁷. However, considering that the Notification does not include additional rules per se but rather clarifications on how the statutory text of PIPA should be understood to apply and in light of its overall importance particularly with respect to the pseudonymisation provisions under PIPA which the EDPB understands are the object of ongoing judicial cases, the EDPB invites the European Commission to provide further information on the binding nature, the enforceability and validity of Notification No 2021-1 and would recommend an attentive monitoring of its respect in practice, in particular with regard to its application not only by the Korean supervisory authority but also by courts, especially where the equivalent level of protection afforded by the Korean legal framework is based on the clarifications provided for therein.

⁷ See Section I of Annex I of the draft decision.

1.2.2. General data protection aspects

11. In relation to the scope of application of the adequacy decision, the EDPB notes that it will cover transfers from the EEA legal framework to both, public and private “personal information controllers” falling under the scope of the PIPA. The EDPB understands that entities acting as processors within the meaning of the GDPR are included in this term, however, in order to avoid misunderstandings, it invites the European Commission to make it clearer that the adequacy decision will also cover transfers to “processors” in Korea.
12. An important aspect that the EDPB would like to call the attention to relates to the concept of pseudonymised information in the Korean data protection framework. Under Korean law, exemptions from a number of relevant provisions, including those on individual data subject rights and data retention, apply to the processing of pseudonymised personal information. According to the European Commission, this is only the case where pseudonymised personal information is processed for the purposes of statistics, scientific research or archiving in the public interest. However, this assertion is mainly supported by Notification No 2021-1 which makes the already mentioned need for additional information about and the monitoring of the binding nature, enforceability and validity of this Notification highly relevant in this context. In addition, the EDPB invites the European Commission to further assess the impact of pseudonymisation under Korean law and, most importantly, how it may affect the fundamental rights and freedoms of data subjects whose personal data is transferred to the Republic of Korea under the adequacy decision. In particular, the EDPB calls on the European Commission to assess further the derogations contained in Article 28(7) PIPA and Article 40(3) CIA and to attentively monitor their application and relevant case law in order to ensure that the data subject rights are not be unduly restricted when personal data transferred under the adequacy decision is processed for these purposes.
13. Further, the EDPB notes that under Korean law a right to withdraw consent exists only in specific circumstances and therefore invites the European Commission to further assess the impact of a lack of a general right to withdraw consent and to provide further assurances so as to ensure than an essential level of data protection is guaranteed at all times also, where necessary, by clarifying the role of the right to suspension under PIPA in the absence of a general right to withdraw consent.
14. With regard to onward transfers, the EDPB acknowledges that informed consent of the data subject will be generally used as a basis for data transfers from a Korean-based personal information controller to a third country-based recipient and that Notification No 2021-1 envisages that individuals must be informed about the third country to which their data will be provided. However, the EDPB invites the European Commission to ensure that the information to be provided to the data subject also includes information on the possible risks of transfers arising from the absence of adequate protection in the third country as well as the absence of appropriate safeguards. Furthermore, the EDPB would welcome reassurances in the adequacy decision that personal data will not be transferred from Korean personal information controllers to a third country in any situation in which under the GDPR valid consent could not be provided, e.g. because of an imbalance of power.
15. With regard to the appointment of the members of the Korean supervisory authority, although the formal procedure would be in line with GDPR and therefore meet the test of equivalence with the EEA legal framework, the EDPB would welcome the European Commission to monitor any developments that might affect the independence of the members of the South Korean supervisory authority.
16. Regarding the budget, again based on the information provided by the European Commission, no reference is made to the specificities of the staff assigned to the PIPC nor to the financial resources made available to it. The EDPB would therefore welcome additional information in the draft decision on these two relevant topics.

1.2.3. On the access by public authorities to data transferred to the Republic of Korea

17. The EDPB has also analysed the Korean legal framework with respect to government access for law enforcement and national security purposes to personal data transferred from the EEA to Korea. While acknowledging the representations and assurances provided by the Korean government, as outlined in Annex II of the draft decision, the EDPB has identified a number of aspects that require clarification or raise concerns.
18. The EDPB notes that PIPA's provisions apply without limitation in the area of law enforcement. The EDPB also notes that data processing in the area of national security is subject to a more limited set of provisions enshrined in PIPA.
19. With regard to the voluntary disclosure of personal information by telecommunication providers to national security authorities the EDPB is concerned that the relationship of Section 3 of Annex I of the draft decision which specifies that providers in principle have to notify the concerned individual when they voluntarily comply with a request, and Article 58(1) lit. 2 PIPA, i.e., the partial exemption for national security purposes, is unclear. This could render information requirements ineffective, making it considerably more difficult for data subjects to assert their data protection rights especially with regard to judicial redress.
20. While the draft decision does not explicitly say so, the EDPB understands from the explanations provided by the European Commission that the Korean legal framework does not allow for the interception of telecommunication data in bulk. Therefore, the recent case law of the European Court of Human Rights ("ECtHR") on bulk interception regimes would not be directly relevant for the assessment of the level of data protection in Korea.
21. The draft decision does not contain any information on the legal framework for onward transfers in the area of national security. While the EDPB understood that, in the view of the European Commission, onward transfers for national security purposes are sufficiently regulated by the general safeguards and principles following from the constitutional framework and PIPA, the EDPB is concerned as to whether this can be considered to meet the requirements of preciseness and clarity of the law and enshrines effective and enforceable safeguards. The safeguards the European Commission refers to are of a very general nature and do not address, in a legal basis, the specific circumstances and conditions under which onward transfers for national security purposes may take place. In this context, the EDPB also notes that the European Commission did not consider the existence of international agreements concluded between the Republic of Korea and third countries or international organisations that may provide for specific provisions for the international transfer of personal data by law enforcement and/or intelligence services to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of law enforcement or intelligence cooperation is likely to affect the Korean data protection legal framework as assessed.
22. The EDPB notes that the oversight of criminal law enforcement as well as national security authorities is ensured by a combination of different internal and external bodies, in particular the PIPC, which is endowed with sufficient executive powers.
23. Effective remedies and redress require that data subjects are able to turn to a competent body that meets the requirements of Article 47 of the Charter of Fundamental rights of the European Union ("**the Charter**"), i.e., which is competent to determine that a data processing is taking place, to verify the lawfulness of the processing, and which has enforceable remedial powers in the event the data processing is unlawful. Against this background, the EDPB asks the European Commission to clarify whether a complaint with the PIPC or any action before a court is subject to substantive and/or procedural requirements, such as a burden of proof, and whether individuals in the EEA would be able to meet such precondition.

1.3. Conclusion

24. The EDPB considers that this adequacy decision is of paramount importance also taking into account that – with the exceptions highlighted in the opinion – it will cover transfers both, in the public and private sector.
25. The EDPB welcomes the efforts made by the European Commission and the Korean authorities to align the Korean legal framework with the European one. The improvements intended to be brought in by Notification No 2021-1 to bridge some of the differences between the two frameworks are very important and well received. However, the EDPB notices that a number of concerns, including with regard to Notification No 2021-1, coupled with the need for further clarifications on other issues, remain, and it recommends the European Commission to address the concerns and requests for clarification raised by the EDPB and provide further information and explanations regarding the issues raised in this opinion.

2. INTRODUCTION

2.1. Korean data protection framework

26. The main piece of legislation governing data protection in the Republic of Korea is the Personal Information Protection Act (Act No. 10465 of 29 March 2011, last amended by Act No. 16930 of 4 February 2020, “**PIPA**”). It is supplemented by an Enforcement Decree (Presidential Decree No. 23169 of 29 September 2011, last amended by Presidential Decree No. 30892 of 4 August 2020, “**PIPA Enforcement Decree**”), which is legally binding and enforceable.
27. In addition to PIPA, the Korean data protection framework includes regulatory “Notifications” issued by the Korean supervisory authority, the Personal Information Protection Commission (“**PIPC**”), providing further rules on the interpretation and application of PIPA. Recently, the PIPC adopted Notification No 2021-1 of 21 January 2021 (which amended the previous Notification No 2020-10 of 1 September 2020, hereafter “**Notification No 2021-1**”) on the interpretation, application and enforcement of certain provisions of PIPA. More specifically, this Notification resulted from adequacy discussions held between Korean authorities and the European Commission. It contains clarifications on the application of specific provisions of PIPA, including concerning the processing of personal data transferred to Korea based on the envisaged adequacy decision⁸ and it *has the status of an administrative rule with legally binding force on the personal information controller in the sense that any violation of th[e] Notification may be regarded as a violation of the relevant provisions of PIPA*⁹. In this context, the EDPB would like to note that, despite being referred to as “Supplementary Rules” in the draft decision, the Notification does not include additional rules *per se* but rather explanations aimed at clarifying how the statutory text of PIPA should be understood to apply, in particular with respect to data transferred from the EEA. Against this background, the EDPB would recommend an attentive monitoring of the respect of Notification No 2021-1 in practice, in particular with regard to their application not only by the PIPC but also by courts, especially where the equivalent level of protection afforded by the Korean legal framework is based on the clarifications provided for in the Notification No 2021-1.
28. Other relevant data protection laws in the Korean legislative framework lay down rules to the processing of personal data in specific industry sectors such as:
 - The Act on the Use and Protection of Credit Information (“**CIA**”), including its Enforcement Decree (“**CIA Enforcement Decree**”), which lay down specific rules applicable to

⁸ See Section I of Annex I of the draft decision.

⁹ Ibid.

- commercial operators and specialised entities (such as credit rating agencies, financial institutions) when they process personal credit information necessary to determine the creditworthiness of parties to financial or commercial transactions;
 - The Act on the Promotion of Information and Communications Network Utilisation and Data Protection (“**Network Act**”); and
 - The Communications Privacy Protection Act (“**CPPA**”)
29. In the area of government access, apart from the relevant provisions contained in the PIPA and the CPPA, the EDPB has considered some other pieces of legislation, i.e., the Criminal Procedure Act (“**CPA**”), the Telecommunications Business Act (“**TBA**”), the Act on Reporting and Using Specified Financial Transaction Information (“**ARUSFTI**”) and the National Intelligence Service Act (“**NISA**”).

2.2. Scope of the EDPB’s assessment

30. The draft decision of the European Commission is the result of an assessment of the Korean data protection framework, followed by discussions with the Korean government. In accordance with Article 70(1)(s) GDPR, the EDPB is expected to provide an independent opinion on the European Commission’s findings, identify insufficiencies in the adequacy framework, if any, and endeavour to make proposals to address these.
31. In order to avoid repetition and with the aim to help in the assessment of the Korean legal framework, the EDPB has chosen to focus on some specific points presented in the draft decision and provide its analysis and opinion on them, refraining from reproducing most of the factual findings and assessments where the EDPB has no indication to assume that the law of the Republic of Korea would not be essentially equivalent to the law in the EEA. In addition, in line with the jurisprudence of the CJEU, a very important part of the analysis covers the legal regime of national security access to the personal data transferred to the Republic of Korea, and the practice of its national security apparatus.
32. In its assessment, the EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the Charter, respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial, and Article 8 ECHR protecting the right to private and family life. In addition to the above, the EDPB considered the requirements of the GDPR as well as the relevant case law.
33. The objective of this exercise is to provide the European Commission with an opinion on the assessment of the adequacy of the level of protection in the Republic of Korea. The concept of “adequate level of protection” which already existed under Directive 95/46, has been further developed by the CJEU. It is important to recall the standard set by the CJEU in Schrems I, namely that – while the “level of protection” in the third country must be “essentially equivalent” to that guaranteed in the EU – *“the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU”*¹⁰. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process personal data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness

¹⁰ C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October 2015, ECLI:EU:C:2015:650, paras. 73-74.

of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules¹¹.

2.3. General comments and concerns

2.3.1. International commitments entered into by the Republic of Korea

34. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential¹², when assessing the adequacy of the level of protection of a third country, the European Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations.
35. Korea is a party to several international agreements that guarantee the right to privacy, such as the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of Persons with Disabilities (Article 22) and the Convention on the Rights of the Child (Article 16). Furthermore, Korea, as an OECD member, adheres to the OECD Privacy Framework, in particular the Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data.
36. The EDPB also takes note of the participation of Korea as Observer State in the work of the Consultative Committee of the Council of Europe Convention 108(+), although it has not yet decided whether to accede.

2.3.2 Scope of the adequacy decision

37. According to Recital 5 of the draft decision, the European Commission concludes that the Republic of Korea ensures an adequate level of protection for personal data transferred from a controller or processor in the Union to personal information controllers (e.g. natural or legal persons, organisations, public institutions) falling within the scope of application of PIPA, with the exception of processing of personal data for missionary activities by religious organisations and for the nomination of candidates by political parties¹³, or the processing of personal credit information pursuant to the CIA by controllers that are subject to oversight by the Financial Services Commission.
38. The EDPB notes that the adequacy decision will cover transfers from the EEA legal framework to both, public and private "personal information controllers" falling under the scope of the PIPA. The EDPB understands that entities acting as processors within the meaning of the GDPR are also covered by the term "personal information controller" considering that the PIPA will apply equally to them and that specific obligations apply when a personal information controller (the "outsourcer") engages a third party for the processing of personal information (the "outsourcee"), however, in order to avoid misunderstandings, the EDPB invites the European Commission to make it clearer that the adequacy decision will also cover transfers to "processors" in Korea and that the level of protection of personal data transferred from the EEA will not be undermined also in these cases.
39. Besides, taking into account that the adequacy decision also covers personal data transfers between public bodies, the EDPB understands that this will also cover transfers between data protection supervisory authorities and, for the sake of clarity, invites the European Commission to specifically address this issue.

¹¹ WP254, p.2.

¹² WP254, p.2.

¹³ For more context see below under section 3.1.2 of this opinion.

- 40. Furthermore, with regards to the entities excluded from the scope of application of the adequacy decision, the EDPB would like to emphasise that the adequacy decision could benefit from a clearer identification of the “commercial organisations” that are subject to the oversight of the PIPC (Article 45(3) CIA) so that EEA-based controllers and processors may easily assess whether the importer falls also under the scope of application of the adequacy decision before transferring data to entities falling under the scope of application of the CIA or, at least, be alerted of the need to assess this aspect.
- 41. With respect to the scope of the adequacy decision, the EDPB understood from the additional explanations of the European Commission that the Korea Financial Intelligence Unit (“**KOFIU**”), which is established under the Financial Services Commission and oversees the prevention of money laundering and terrorist financing pursuant to the ARUSFTI¹⁴, is also excluded from the scope, as it has only jurisdiction over financial institutions which are themselves not covered by the draft decision. However, Article 1(2)(c) of the draft decision excludes from its scope only those personal information controllers that are subject to oversight by the Financial Services Commission and process personal credit information under the CIA. Against this background, the EDPB asks the European Commission to clarify whether the KOFIU and the data processing activities undertaken by KOFIU itself fall under the draft decision.

3. GENERAL DATA PROTECTION ASPECTS

3.1. Content principles

- 42. Chapter 3 of the GDPR Adequacy Referential is dedicated to the “Content Principles”. A third country’s system must contain them in order to regard the level of protection provided as essentially equivalent to the one guaranteed by EU legislation.
- 43. Although the right to the protection of personal data is not expressly enshrined in the Korean Constitution per se, it is recognised as a basic right, derived from the constitutional rights to human dignity and the pursuit of happiness (Article 10), private life (Article 17) and privacy of communications (Article 18). This has been confirmed by both, the Supreme Court and the Constitutional Court, as referenced in the European Commission’s draft decision¹⁵. The EDPB takes notes of this recognition since it derives from it that data protection as a basic right, according to Article 37 of the Korean Constitution, *“may only be restricted by law and when necessary for national security, or the maintenance of law and order or for public welfare”* and that *“even when such restrictions are imposed, they may not affect the essence of the freedom or right”*.
- 44. According to the European Commission¹⁶, the Constitutional Court has ruled that also foreign nationals are the subject of basic rights. As per the official representations from the Korean government¹⁷, although case law has so far not specifically dealt with the right to privacy by non-Korean nationals, it is widely accepted among scholars that Articles 12-22 of the Constitution set out “rights of human beings”. Further, the Republic of Korea has enacted a series of laws in the area of data protection that provide safeguards for all individuals, irrespective of their nationality, such as the PIPA. In this regard, the EDPB takes note that Article 6(2) of the Constitution provides that the status of foreign nationals is guaranteed as prescribed by international law and treaties and of the case law mentioned in the draft decision according to which a “foreigner” can be the bearer of “basic rights”. Considering the relevance of the recognition of the right to data protection to “foreign nationals”, the EDPB calls the attention of the European Commission on the need to keep monitoring the case law

¹⁴ See Annex II, section 2.2.3.1.

¹⁵ See Recital 8 of the draft decision and the relevant case law referred to in footnote 10 of the draft decision of which only English summaries are available.

¹⁶ See Recital 9 of the draft decision.

¹⁷ Section 1.1. of Annex II of the draft decision.

relating to data protection as a basic right recognised not only to Korean citizens but to all data subjects so as to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data are transferred to Korea under the adequacy decision.

3.1.1. Concepts

45. Based on the GDPR Adequacy Referential, basic data protection concepts and/or principles should exist in the third country's legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in the European data protection law. For example, the GDPR includes the following important concepts: "personal data", "processing of personal data", "data controller", "data processor", "recipient" and "sensitive data"¹⁸.
46. The PIPA includes a number of definitions such as, among others, those of "personal information", "processing" and "data subject", which closely resemble the corresponding terms under the GDPR.

3.1.1.1. Concept of pseudonymised data

47. Among the definitions provided in the PIPA, Article 2(1) PIPA defines, in particular, personal information as any of the following information relating to a living individual: (a) information that identifies a particular individual by his or her full name, resident registration number, image, etc. and (b) information which, even if it by itself does not identify a particular individual, may easily be combined with other information to identify a particular individual. In the latter cases, whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual such as the likelihood that the other information can be procured.
48. In addition, according to Article 2(1) lit. (c) PIPA, also "pseudonymised information" is considered personal information. Pseudonymised information is defined as information under items (a) or (b) above that is pseudonymised in accordance with subparagraph 1-2 and thereby becomes incapable of identifying a particular individual without the use or combination of information for restoration to the original state. Information that is fully anonymised is excluded from the scope of application of the PIPA. According to Article 58(2) PIPA, the act does not apply to information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc.
49. The European Commission states in Recital 17 of its draft decision that this corresponds with the material scope of application of the GDPR and its notions of "personal data", "pseudonymisation" and "anonymised information".
50. However, according to Article 28(7) PIPA, Articles 20, 21, 27, 34(1), 35 through 37, 39(3), 39(4), 39(6) through 39(8) do not apply to pseudonymised personal information.
51. In its draft decision, the European Commission states that Article 28(7) PIPA is only applicable to pseudonymised personal information when it is processed for the purposes of statistics, scientific research or archiving in the public interest¹⁹. However, this does not follow directly from the letter of the law but from the explanations provided in Notification No 2021-1²⁰. While the EDPB acknowledges that an argument can be made based on the structure and rationale of PIPA that Article 28(2) PIPA should be understood and logically interpreted as also applying to Article 28(7) PIPA, in light of the importance of Notification No 2021-1 in the European Commission's assessment of the adequacy of the level of protection of personal data in the Republic of Korea and to avoid any doubt, the EDPB

¹⁸ WP254, p. 4.

¹⁹ See *inter alia* Recital 82 of the draft decision.

²⁰ Section 4 of Annex I to the draft decision.

invites the European Commission to provide further information on the binding nature, enforceability and validity of Notification No 2021-1 and to monitor its application in this specific context.

52. In this context, the EDPB would like to recall that under the GDPR pseudonymisation is understood as a recommended security measure. In other words, under the GDPR pseudonymised data remains personal data to which the GDPR fully applies. Based on the foregoing, the EDPB has concerns that the GDPR's level of protection of pseudonymised personal data could be undermined when personal data are transferred to Korea. The EDPB therefore invites the European Commission to further assess the impact of pseudonymisation under the PIPA and, most importantly, how it may affect the fundamental rights and freedoms of data subjects whose personal data would be transferred to the Republic of Korea on the basis of the adequacy decision. Hence, the EDPB calls upon the European Commission to provide assurances that the level of protection of personal data from data subjects in the EEA will not be lowered after transfer to the Republic of Korea even where the personal data transferred is pseudonymised.

3.1.1.2. Concept of personal information controller

53. Article 2(5) PIPA includes a definition of "personal information controller" meaning a public institution, legal person, organisation or individual, etc. that processes personal information directly or indirectly to operate personal information files "*as part of its activities*". However, in the additional safeguards set out in Notification No 2021-1, the term personal information controller is defined as a public institution, legal person, organisation, individual etc. that processes personal information directly or indirectly to operate the personal information files "*for business purposes*". Instead, footnote 272 of the draft decision states the following about the notion of personal information controller: "*As defined in Article 2 PIPA, i.e. a public institution, legal person, organisation, individual, etc. that processes personal information directly or indirectly to operate personal information files 'for official or business purposes'.*"
54. The EDPB acknowledges that these inconsistencies may be due to the translations of the original text as provided by the Korean authorities and invites the European Commission to verify the quality and certainty of the translations regularly. However, the EDPB stresses the fact that, in order to be able to assess the essential equivalence of the level of data protection of the Korean legal framework, a clear understanding of the processing purposes falling within the material scope PIPA is required. Further, in this context, the EDPB notes that the PIPA does not use the same terminology of the GDPR in relation to the notion of "controller" and "processor" and invites the European Commission to clarify the correct definition and scope of the concept of "personal information controller" and to specifically address whether this term also covers processors within the meaning of the GDPR, as this directly affects the scope of the adequacy decision²¹.

3.1.2. Partial exemptions provided for in PIPA

55. Article 58(1) PIPA excludes the application of parts of PIPA (i.e., Articles 15 to 57) with respect to four categories of personal data processing as described below. Specifically, the exemptions relate to the provisions of PIPA on specific grounds for processing, certain data protection obligations, the detailed rules for the exercise of individual rights as well as the rules governing dispute resolution. However, the EDPB takes note that some general provisions of PIPA still remain applicable, such as those relating to the data protection principles (Article 3 PIPA) and individual rights (Article 4 PIPA). In addition, Article 58(4) PIPA sets out specific obligations on those four categories of data processing.
56. Firstly, the partial exemption covers personal information collected pursuant to the Statistics Act for processing by public institutions. The European Commission states in Recital 27 of its draft decision

²¹ See also para. 38 above.

that according to clarifications received from the Korean government, personal data processed in this context normally concerns Korean nationals and might only exceptionally include information on foreigners, namely in the case of statistics on entry to and departure from the territory, or on foreign investments. According to the draft decision, however, even in these situations, such data is normally not transferred from controllers/processors in the EEA but would rather be directly collected by public authorities in Korea.

57. The EDPB acknowledges the reasoning of the European Commission on the exceptionality of the application of the Statistics Act to the processing of personal data transferred under the adequacy decision; however, it would welcome further information and reassurances about the specific safeguards that would be applied in case personal data transferred from the EEA is further collected pursuant to the Statistics Act for processing by public institutions, in particular relating to the exercise of individual rights by data subjects in line with Article 89(2) GDPR in so far as such rights are not likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are not necessary for the fulfilment of those purposes.
58. In this perspective, the application of Article 4 PIPA also to this kind of processing appears to provide reassurances, however the EDPB would welcome additional information and clarifications in the adequacy decision on the specific obligations imposed, in accordance with Article 58(4) PIPA, on those processing activities, namely with respect to data minimisation, limited data retention, security measures and the handling of complaints.
59. Secondly, the partial exemption covers personal information collected or requested to be provided for the analysis of information related to national security. The EDPB is aware of the fact that in matters of national security, states have a broad margin of appreciation recognized by the ECtHR. The EDPB also notes that, according to Article 37(2) of the Korean Constitution, any restriction to the freedoms and rights, for example, when necessary for the protection of national security, may not violate the essential aspect of that freedom or right. Further, the EDPB notes the safeguards in Section 6 of Notification No 2021-1 regarding the processing of personal information for national security purposes including investigation of infringements and enforcement. However, in this context, the EDPB calls on the European Commission to clarify further the scope of the exemptions as it wonders whether all of the exemptions provided under Article 58(1) lit. 2 PIPA (Chapters III through VII) are relevant for the work of intelligence services, and whether they ensure equivalence with the necessity and proportionality principles. In particular, the EDPB invites the European Commission to provide more clarification regarding under which circumstances an intelligence service could rely on the exemptions. The EDPB considers it necessary to closely monitor the impact of these limitations in practice, especially on the effective exercise and enforcement of data subject rights.
60. Thirdly, the partial exemption applies to "*personal information processed temporarily where it is urgently necessary for public safety and security, public health, etc.*" According to Recital 29 of the European Commission's draft decision, this category is interpreted strictly by the PIPC and applies only in emergencies requiring urgent action, for example, to track infectious agents, or to rescue and aid victims of natural disasters.
61. The EDPB also emphasizes that any derogations to the level of protection for personal data should be interpreted strictly. At the same time, the EDPB notes that the provision is not strictly defined and does not provide an exhaustive list of examples of situations where the processing of personal information might be considered "*urgently necessary*". For example, the EDPB is concerned as to whether international transfers of health data during the ongoing COVID-19 pandemic would also fall within the scope of this exemption. In the light of above, the EDPB calls on the European Commission to provide further clarifications on the scope of this exemption and to fully monitor its application and scope to ensure that it does not lead to the level of protection of personal data from the EEA being lowered after transfer to Korea on the basis of the adequacy decision.

62. Finally, the partial exemption applies to personal information collected or used for the purposes of reporting by the press, missionary activities by religious organizations, and nomination of candidates by political parties²². With respect to the processing of personal information by the press for journalistic activities, the European Commission states in Recital 31 of its draft decision that the balancing between freedom of expression and other rights, including the right to privacy, is provided by the Act on Arbitration and Remedies, etc. for Damage Caused by Press Reports (hereafter “**Press Act**”), and presents specific safeguards that follow from the Press Act. The EDPB would, however, call on European Commission to fully monitor this exemption and the relevant case law in order to ensure that an equivalent level of data protection is ensured also in practice in the Korean legal framework.

3.1.3 Grounds for lawful and fair processing for legitimate purposes

63. According to the GDPR Adequacy Referential, in line with the GDPR, data must be processed in a lawful, fair and legitimate manner. The legal basis, under which personal data may be lawfully, fairly and legitimately processed should be set out in a sufficiently clear manner. The European framework acknowledges several such legitimate grounds including for example, provisions in national law, the consent of the data subject, performance of a contract or legitimate interests of the data controller or of a third party which does not override the interests of the individual.
64. Following a similar structure as the GDPR, PIPA first introduces the principle of lawfulness, fairness and transparency at the beginning (Article 3(1) and (2) PIPA), laying out the specific rules for its application later on (Articles 15 to 19 PIPA). Specifically, Article 15 PIPA includes a catalogue of legal grounds on which personal information controllers may base the collection of personal information and use it within the scope of the purpose collection. These legal grounds consist of (1) the data subject’s informed consent; (2) statutory authorization or necessity for compliance with a legal obligation; (3) necessity for the performance of a public institution’s duties; (4) necessity for the execution or performance of a contract with a data subject; (5) necessity for the protection of life, bodily or property interests of the data subject or a third party from imminent danger (and prior consent cannot be obtained); (6) necessity to attain a justifiable interest of a personal information controller which is superior to that of a data subject.
65. In addition, Article 17 PIPA lists the legal grounds applicable for sharing personal information with a third party which include (1) the data subject’s informed consent; (2) statutory authorization or necessity for compliance with a legal obligation; (3) necessity for the performance of a public institution’s duties; and (4) necessity for the protection of life, bodily or property interests of the data subject or a third party from imminent danger (and prior consent cannot be obtained). Even in the absence of the data subject’s consent, the sharing of personal information is allowed where this occurs within the scope reasonably related to the purposes for which the personal information was initially collected (Article 17(4) PIPA).
66. Article 18 PIPA lays down specific rules for the use and sharing of personal information where this occurs out of the scope of the initial purpose of collection or provision. Among other, here too, consent is one such authorizing rule.
67. While acknowledging the substantial similarity of Korean law to the GDPR with respect to the principle of lawfulness and the existence of a general right to suspension (Article 37 PIPA), which can also be invoked where personal data is processed on the basis of consent, the EDPB would like to note the

²² Accordingly, the processing of personal information by religious organisations for their missionary activities and the processing of personal information by political parties in the context of the nomination of candidates are also excluded from the scope of the adequacy decision. See also para. 37 above in section 2.3.2.

absence of a general right to withdraw consent under PIPA²³. In light of the importance of consent as a legal ground in all of the above-described scenarios, and taking into consideration the role of individual rights in a data protection legal system for the purposes of safeguarding the data subjects' fundamental rights and freedoms, the EDPB invites the European Commission to further assess the impact of the lack of a general right to withdraw consent under Korean law and to provide further assurances to ensure that an essential level of data protection as the one provided for under the GDPR is guaranteed at all times also, where necessary, by clarifying the role of the right to suspension in this specific context.

3.1.4 The purpose limitation principle

68. The GDPR Adequacy Referential, in line with the GDPR, provides that personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.
69. Pursuant to Article 3(1) and (2) PIPA, personal information controllers shall specify and explicit the purposes of processing and ensure that the processing is compatible with these purposes. While this principle is confirmed in other provisions (i.e., Articles 15(1), 18(1) and 19(1) PIPA), processing for "reasonably related" purposes is allowed in certain circumstances (see Article 17(4) PIPA)²⁴ as well as the out-of-purpose use and provision of personal information (see Articles 18 and 19 PIPA)²⁵.
70. The EDPB understands that in case of transfers of personal data from the EEA to the Republic of Korea on the basis of the adequacy decision, the purpose of collection of the EEA-based controllers constitutes the purpose for which the data is transferred applicable to the processing by the receiving Korean-based personal information controller. A change of purpose by the Korean-based controller would only be allowed as provided for in Article 18(2) lit. 1-3 PIPA, "*unless doing so is likely to unfairly infringe on the interest of a data subject or a third party*"²⁶. In this context, the EDPB acknowledges the European Commission's statement in Recital 55 of the draft decision that, where changes of purpose are authorised by law, such laws have to respect the fundamental right to privacy and data protection. However, the EDPB notes that no specific information has been provided to sustain this particular statement, for example, no reference has been made to Article 37 of the (Korean) Constitution. Therefore, the EDPB calls on the European Commission to provide further assurances and guarantees in the draft decision to ensure that any laws authorizing a change of processing purpose are required to respect the fundamental rights and freedoms of data subjects to privacy and data protection.

3.1.5 The data quality and proportionality principle

71. The GDPR Adequacy Referential states that data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.

²³ Even though data subjects may deny consent in certain circumstances, see for example Article 18(3) 5 PIPA. By contrast, the right to withdraw consent seems to exist only in specific cases ; pursuant to Article 27(1) 2 PIPA data subjects have the right to withdraw consent where they do not wish their personal information to be transferred to a third party owing to the transfer of some or all of the personal information controller's business, a merger, etc.; pursuant to Article 39(7) PIPA users may withdraw consent to the collection, use and provision of personal information at any time from information and communications service provider, etc.; and pursuant to Article 37 CIA an individual credit information subject may revoke the consent which had been provided to a credit information provider/user.

²⁴ Whereby purpose compatibility must be ascertained in advance on the basis of the criteria laid down in Article 14-2 PIPA Enforcement Decree.

²⁵ See also above under para. 66.

²⁶ Article 18(2) PIPA.

72. Under PIPA, personal information controllers must ensure that personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed (Article 3(3) PIPA). Personal information controllers are required to collect as little personal information as necessary to achieve a given purpose. They bear the burden of proof in this regard (Article 16(1) PIPA).
73. Against this background, the EDPB shares the European Commission's assessment with respect to the essential equivalence of the level of protection under PIPA vis-à-vis the GDPR in this regard.

3.1.6 Data retention principle

74. According to the GDPR Adequacy Referential, as a general rule data should be kept for no longer than is necessary for the purposes for which the personal data is processed. As per Article 21(1) PIPA, this principle exists in Korean law as well. Under PIPA, personal information controllers are required to destroy personal information without delay when the personal information becomes unnecessary upon expiry of the retention period or upon achievement of the intended purpose of processing, unless statutory retention periods apply.
75. The EDPB is, however, concerned as to the fact that Article 21(1) PIPA is not applicable to pseudonymised personal information. The EDPB takes note of the fact that, according to Section 4(iii) of Notification No 2021-1, “[w]here a personal information controller processes pseudonymised information for the purpose of compiling statistics, scientific research, preservation of public records, etc. and if the pseudonymised information has not been [sic] destroyed once the specific purpose of processing has been fulfilled in line with Article 37 of the Constitution and Article 3 (Principles for Protecting Personal Information) of the Act, it shall anonymise the information with a view to ensure that it no longer identifies a specific individual, alone or when combined with other information, reasonably considering time, cost, technology, etc., in accordance with Article 58(2) PIPA.” Given, here too, the importance of Notification 2021-1 and with a view to having legal certainty as to the equivalence of the level of protection of personal data transferred to the Republic of Korea under the adequacy decision, the EDPB reiterates its call on the European Commission to provide further information specifically on how Notification No 2021-1 is made binding and its enforceability and validity is ensured²⁷.

3.1.7 The security and confidentiality principle

76. As described in the GDPR Adequacy Referential, the security and confidentiality principle requires data processing entities to make sure that personal data is processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organisational measures. The level of the security should take into consideration the state of the art and the related costs.
77. The European Commission has identified a similar principle of data security in Article 3(4) PIPA, which is further specified in Article 29 PIPA. In addition, data security provisions apply where the personal information controller engages an “outsourcer”. The security of the processing must be ensured through technical and managerial safeguards, which must also be included in the binding data processing agreement (Article 26 PIPA and Article 28 PIPA Enforcement Decree). Further, under PIPA specific obligations apply in the event of a data breach, including the obligation to notify affected data subjects and the supervisory authority where the number of affected data subjects exceeds the applicable threshold (Article 34 PIPA in conjunction with Article 39 PIPA Presidential Decree), except where the affected data is pseudonymised personal information processed for the purposes of

²⁷ See also above para. 51 under section 3.1.1.1 of this opinion, as well as para. 52 for the EDPB's general concerns regarding the impact of pseudonymisation under Korean law.

statistics, scientific research or archiving in the public interest (Article 28(7) PIPA). Here, too²⁸, the EDPB is concerned with the wide reaching exemptions for pseudonymised information and reiterates its call on the European Commission to further assess this aspect to ensure that a level of protection essentially equivalent is provided for under Korean law²⁹.

78. Notwithstanding, in sum, the EDPB is satisfied with the European Commission's assessment and conclusion regarding the essential equivalence of Korean law with respect to the principle of security and confidentiality.

3.1.8 The transparency principle

79. Based on Article 5(1)(a) GDPR, transparency is a fundamental principle of the EU data protection system. Recital 39 GDPR outlines the crucial function of this principle by stating that "*[i]t should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. (...) Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.*"
80. The GDPR Adequacy Referential explicitly names "transparency" as one of the content principles to be taken into account when evaluating the essential equivalence of the level of protection provided for by a third country. More specifically, it states that "*[e]ach individual should be informed of all the main elements of the processing of his/her personal data in a clear, easily accessible, concise, transparent and intelligible form. Such information should include the purpose of the processing, the identity of the data controller, the rights made available to him/her and other information insofar as this is necessary to ensure fairness. Under certain conditions, some exceptions to this right for information can exist, such as for example, to safeguard criminal investigations, national security, judicial independence and judicial proceedings or other important objectives of general public interest as is the case with Article 23 GDPR.*"
81. Similarly as is the case with the GDPR, under PIPA a general transparency principle exists requiring personal information controllers to make public their privacy policy and other matters related to personal information processing (Article 3(5) PIPA). Specific information obligations apply where personal information controllers seek to obtain consent from the data subjects for the collection and processing of personal information (Article 15(2) PIPA), for the sharing of personal information with a third party (Article 17(2) PIPA) and for out-of-purpose processing (Article 18(3) PIPA). It is noteworthy that these information obligations also apply *mutatis mutandis* to the outsourcee (Article 26(7) PIPA).
82. The EDPB acknowledges and welcomes the additional safeguards in Section 3(i) and (ii) of Notification No 2021-1³⁰ relating to information to be provided to data subjects when their data are transferred by an EEA entity taking into account the fact that pursuant to Article 20(1) PIPA, when data has not been obtained from the data subject, data subjects are informed only upon request while a general right to be informed is only recognized pursuant to Article 20(2) PIPA where certain processing operations exceed thresholds set forth in the PIPA Enforcement Decree (Article 15(2)).
83. Overall, the EDPB is satisfied that the level of protection under Korean law with respect to the transparency principle is essentially equivalent to that provided under the GDPR.

²⁸ As already laid down in paras. 51-52 above and section 3.1.1.1 of this Opinion.

²⁹ See also sections 3.1.6 and 3.1.10 of this Opinion.

³⁰ Annex I of the draft decision.

3.1.9 Special categories of personal data

84. For a third country's data protection system to be recognized as providing a level of protection of personal data essentially equivalent to that of the GDPR, specific safeguards should exist where special categories of personal within the meaning of Articles 9 and 10 GDPR are involved.
85. Under PIPA, specific provisions apply to the processing of so-called sensitive information, which includes personal information revealing the ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject, as well as, by reference to the PIPA Enforcement Decree, DNA information acquired from genetic testing, data that constitutes a criminal history record; personal information resulting from specific technical processing of data relating to the physical, physiological or behavioural characteristics of an individual for the purpose of uniquely identifying that individual; and personal information revealing racial or ethnic origin.
86. Similarly to the GDPR, Korean data protection law prohibits the processing of sensitive information unless specific exemptions apply consisting of (1) informing the data subject and obtaining a specific consent and (2) legal provisions authorizing the processing (Article 23(2) PIPA).
87. On this basis, the EDPB in principle agrees with the European Commission's conclusion of essential equivalence of Korean law with respect to the processing of special categories of personal data. However, the EDPB would like to note that it has not been provided with the PIPA Handbook nor with the clarifications from the PIPC with regard to the term "sexual life" being interpreted as also covering the individual's sexual orientation or preferences, which have not been included in Notification No 2021-1. The EDPB therefore calls on the European Commission to provide this information to be able to independently assess it. Further, the EDPB invites the European Commission to specifically cite the documents where the information it refers to on this topic can be found.

3.1.10 Rights of access, rectification, erasure and objection

88. In the Korean legal framework, data subject rights are recognized in Article 3(5) PIPA – according to which the personal information controller shall guarantee the data subject rights listed in Article 4 PIPA and further specified in Articles 35 to 37, 39 and 39(2) PIPA and, as for "personal credit information" (i.e., "credit information, that is information that is necessary to determine the creditworthiness of parties to financial or commercial transactions – see Recital 3 of the draft decision), in Articles 37, 38, 38(3) CIA.
89. The EDPB notes that the right of access (and of rectification and erasure which may be exercised by a "*data subject who has accessed his or her personal information pursuant to Article 35*" PIPA) may be limited or denied "*where access is prohibited or limited by Acts*", "*where access may cause damage to the life or body of a third party, or unjustified infringement of property and other interests of any other person*", and in addition, for public institutions, where granting access "*would cause grave difficulties*" in carrying out certain functions, further specified in Article 35(4) PIPA³¹. Similar provisions are also contained in Article 37 PIPA relating to the right of suspension of processing of personal information.
90. Article 23 GDPR allows Union or Member State law to restrict individual rights when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society and envisages such restrictions to safeguard, among others, the protection of the data subject or the rights and freedoms of others and "*a monitoring, inspection or*

³¹ The same conditions and exceptions to the rights of access and correction envisaged by the PIPA apply also with regards to the right of access and correction envisaged for credit personal information by the CIA (footnote 135 of the draft decision).

regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of the same article”.

91. Against this background, the EDPB would welcome general reassurances in the draft decision on the need for any law or statute limiting the rights of the data subjects to meet the requirements of the Korean Constitution that a fundamental right may only be restricted when necessary for national security, or the maintenance of law and order for public welfare, and that this limitation may not affect the essence of the freedom or right concerned (Article 37(2) of the Korean Constitution).
92. Furthermore, with regard to the exception related to “*an unjustified infringement of property or other interests of any other persons*”, the EDPB acknowledges that this “*implies that a balancing should take place between the constitutionally protected rights and freedoms of the individual, on the one hand, and of other persons, on the other hand*”³², however, it would call on the European Commission to fully monitor the application of this exception and the relevant case law in order to ensure that an equivalent level of protection of data subject rights is ensured also in practice in the Korean legal framework.
93. By the same token, the EDPB would welcome an attentive monitoring of the application of the exception for the public bodies, in particular with regard to the cases where granting access would be considered as causing “*grave difficulties*” in performing their duties considering that this expression seems to be broader than the one used in other provisions of the PIPA, e.g. in Article 18(2) lit. 5³³, and should be interpreted restrictively in order to avoid unduly restrictions of the data subject rights.
94. Besides, the EDPB is concerned as to whether the exceptions according to which the provisions regarding transparency on request (Article 20 PIPA) and individual rights (Articles 35 to 37 PIPA) – as well as the similar ones relating to the requirements for information and communication service providers (Article 39(2), 39(6) to 39(8) PIPA) and those contained in the CIA (see exceptions envisaged by Article 40(3) CIA) – do not apply with respect to pseudonymised information, when this is processed for purposes of statistics, scientific research or archiving in the public interest (Article 28(7) PIPA) are in line with the safeguards provided for in the European legal framework.
95. These provisions seem to introduce a general derogation for such kind of processing while the GDPR envisages that, where personal data (including pseudonymised personal data) is processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the data subject rights but only “*in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes*”, pseudonymisation being only one of the technical and organisational measures to be adopted to ensure respect for the principle of data minimization (Article 89(1) GDPR).
96. The European Commission considers the derogation envisaged by Article 28(7) PIPA to be justified also in light of Article 28(5) PIPA by which the personal information controller is expressly prohibited to process the pseudonymised information for the purpose of identifying a certain individual and refers to the approach of Article 11(2) GDPR (in conjunction with Recital 57 GDPR) for processing which does not require identification³⁴.

³² Recital 76 of the draft decision.

³³ In relation to exceptions to the limitation to Out-of-Purpose Use and Provision of Personal Information, Article 18(2) lit. 5 PIPA refers to situations where, for public institutions, “*it is impossible*” to perform the duties.

³⁴ To be noted that the same reasoning would not be applicable as such to the exception envisaged by Article 40(3) CIA for the processing of pseudonymised credit information because Article 40(2)(6) envisages that “*A credit information company, etc. shall not process pseudonymised information in a way that a specific individual*

97. Indeed, according to Article 11 GDPR, the controller shall not be obliged to “*maintain, acquire or process additional information in order to identify the data subject*” for the sole purpose of complying with the GDPR if, for the intended purposes, it may process personal data which do not or do no longer require the identification of a data subject; in such cases, when the controller is able to demonstrate that it is not in a position to identify the data subject, data subject rights do not apply. As acknowledged by the European Commission³⁵, the GDPR therefore requires, in such cases, a “practical” impossibility for the data controller and, in accordance with the principle of data minimization, recognizes that no additional data has to be processed “because of” the GDPR.
98. However, the EDPB deems this situation to be different from the one in which a controller is practically in a position to identify the data subject but it is not allowed to do so by a statutory provision such as the one contained in Article 28(5) PIPA. In this respect, the EDPB welcomes the clarifications provided by the PIPC in the Notification No 2021-1³⁶ confirming that Section 3 PIPA (including Article 28(7)) and the exception of Article 40(3) CIA only apply when pseudonymised information is processed for scientific research, statistics or archiving in the public interest. However – and additionally to the concerns already mentioned about the effective binding nature of the Notification No 2021-1³⁷, the EDPB still wonders whether the derogations envisaged by Articles 28(7) PIPA and Article 40(3) CIA could be considered as necessary and proportionate in a democratic society as far as they restrict the data subject rights in all cases where pseudonymised information is processed for such purposes – i.e., even when the personal information controller is practically in a position to identify the data subject and the rights are not likely to render impossible or seriously impair the achievement of the specific purposes.
99. In particular, the EDPB has concerns that these derogations would not be justified and would need to be further scrutinized especially if applied by the personal information controller that pseudonymises the data “*for statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc.*”, in accordance with Article 28(2) PIPA “*without the consent of data subjects*” (and without providing information envisaged by Article 20 PIPA)³⁸, as far as this controller maintains the information allowing the re-identification. Under the GDPR individuals should be able to exercise their rights with regard to any information which is able to identify or single them out, even if the information is considered “pseudonymised” unless the already mentioned Article 11 GDPR applies. In this respect, the EDPB notes that only when this data is provided to a third party for the same statistical, scientific research purposes and archiving purposes, information that may be used to identify a certain individual should not be included and therefore only the personal information controller to which pseudonymised data is provided according to Article 28-2(2) PIPA would probably be “practically” not in a position to identify the data subject without additional information.
100. In a nutshell, considering that, as recognized by the European Commission, “*instead of relying on pseudonymisation as a possible safeguard, PIPA imposes it as a pre-condition in order to carry out certain processing activities for the purposes of statistics, scientific research and archiving in the public interest (such as to be able to process the data without consent or to combine different datasets)*”³⁹

may be identified for any profit-making or unfair purposes” and could therefore allow re-identification for a fair purpose such as the one to fulfil a data subject request.

³⁵ See Recital 82 of the draft decision.

³⁶ Section 4 of Annex I to the draft decision.

³⁷ See section 3.1.1.1 above.

³⁸ See Article 28(7) PIPA, as explained in the Notification No 2021-1, according to which certain safeguards contained in the PIPA, i.e., “*Articles 20, 21, 27, 34(1), 35 through 37, 39(3), 39(4), 39(6) through 39(8)*”, shall not apply to the pseudonymised information processed for the purpose of compiling statistics, scientific research, preservation of public records, etc.

³⁹ Recital 42 of the draft decision.

but it envisages for such cases important restrictions on the data subjects rights, the EDPB calls on the European Commission to assess further the derogations contained in Article 28(7) PIPA and Article 40(3) CIA and to attentively monitor their application and relevant case law⁴⁰ in order to ensure that the data subject rights will not be unduly restricted when personal data transferred under the adequacy decision is processed for these purposes taking into account that, in many cases, these rights help also the controller to ensure the quality of the processed data.

3.1.11 Restrictions on onward transfers

101. The GDPR Adequacy Referential clarifies that the level of protection of natural persons whose personal data is transferred under an adequacy decision must not be undermined by the onward transfer and therefore any onward transfer “*should be permitted only where the further recipient (i.e., the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller*”.
102. As for the onward transfers to outsourcees (i.e., “processors”) established in other third countries, the EDPB takes note that no special rules are in place in the Korean legal framework to cover these cases and that, as considered by the European Commission⁴¹, a Korean personal information controller has to ensure compliance with PIPA’s provisions on outsourcing (Article 26 PIPA) by means of a legally binding instrument and it will be responsible for the personal information that has been outsourced (Article 26 PIPA).
103. With regards to onward transfers to third parties (i.e., other personal information controllers), according to Article 17(3) PIPA, a Korean personal information controller has to inform the data subjects about and obtain their consent for the overseas transfers and it “*shall not enter into a contract for the cross-border transfer of personal information in violation of the PIPA*”. The EDPB notes that this last provision will ensure – as considered by the European Commission⁴² – that no contract for cross-border transfers could contain obligations contradicting the requirements imposed by PIPA on the personal information controller and could be therefore considered as a safeguard, however, it does not impose any obligation to put in place safeguards to ensure that the same level of protection afforded by the PIPA will be afforded by the recipient. Therefore, the EDPB acknowledges that informed consent of the data subject will generally be used as a basis for data transfers from a Korean-based personal information controller to a third country-based recipient.
104. In this regard, the additional clarifications provided by the PIPC in Notification No 2021-1 regarding the obligation to inform individuals about the third country to which their data will be provided⁴³ are welcomed as this – as highlighted by the European Commission⁴⁴ – would help data subjects in the EEA take a fully informed decision on whether or not to consent to an overseas provision.
105. However, as also considered in the Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, it has to be highlighted that, under the GDPR, data subjects have to be explicitly informed about the possible risks of such transfers arising from the absence of adequate protection in the third country and the absence of appropriate safeguards prior to consent. Such notice should include for example information that there might not be a supervisory authority and/or data processing principles and/or data subject rights

⁴⁰ See, for example, the Open Net’s constitutional challenges (information at <https://opennet.or.kr/19909> available in Korean only).

⁴¹ Recital 87 of the draft decision.

⁴² Recital 88 of the draft decision.

⁴³ Ibid.

⁴⁴ Ibid.

in the third country⁴⁵. For the EDPB, the provision of this information is essential in order to enable the data subject to give an informed consent with full knowledge of these specific facts of the transfer⁴⁶. The EDPB, therefore, has concerns with the European Commission's findings in the draft adequacy decision vis-à-vis this specific kind of transfers. Data subjects are usually not knowledgeable about the data protection framework in third countries. Hence, it cannot be concluded that a data subject could assess the risk of a transfer by only knowing the specific country of destination. There rather has to be a clear information about the specific risks of such a transfer of personal data to a country outside the territory of the Republic of Korea prior to the data subject's consent.

106. Thus, the EDPB invites the European Commission to ensure that the information to be provided to the data subject "*on the circumstances surrounding the transfer*" includes information on the possible risks of the transfer arising from the absence of adequate protection in the third country and of appropriate safeguards. This is important for the EDPB in order to assess whether the consent requirements are essentially equivalent to the GDPR.
107. Furthermore, considering that consent needs to be freely given, informed, specific and unambiguous, the EDPB would welcome reassurances in the adequacy decision that personal data will not be transferred from Korean personal information controllers to a third party in a third country in any situation in which under the GDPR valid consent could not be provided, e.g. because of an imbalance of power.
108. In relation to cases where the personal information controller may provide personal information to a third party overseas without the data subject's consent – i.e., (1) if personal information is provided within the scope reasonably related to the initial purpose of collection according to Article 17(4) PIPA; and (2) if personal information can be provided to a third party in exceptional cases mentioned in Article 18(2) PIPA – the EDPB takes note of the clarifications provided by the PIPC in Section 2 of Notification No 2021-1 (and welcomes the envisaged duty imposed on the Korean-based controller and the overseas recipient to ensure, through a legally binding instrument (such as a contract), a level of protection equivalent to PIPA, including with respect to data subject rights).

3.1.12 Direct marketing

109. According to Articles 21(2) and 21(3) GDPR and the GDPR Adequacy Referential, the data subject has always to be in a position to object without any charge to data processing for purposes of profiling and direct marketing.
110. With regard to the right to suspension envisaged by Article 37 PIPA, the EDPB acknowledges that the European Commission considers that this right also applies where data is used for direct marketing purposes⁴⁷. However, the EDPB would welcome additional information and clarifications in the draft decision in relation to this assessment and, in particular, on the practical application of the right to suspension in the context of direct marketing (e.g. references to relevant case law, etc.). In this respect, the EDPB would also highlight that the right to ask a credit information provider/user to stop contacting him/her for the purpose of introducing or soliciting the purchase of goods or services is explicitly set forth by the CIA (Article 37(2)).
111. Furthermore, as recognized by the European Commission⁴⁸, in the Korean legal framework such processing generally requires the specific (additional) consent of the data subject (see Article 15(1) lit. 1, Article 17(2) lit. 1 of PIPA).

⁴⁵ EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.8.

⁴⁶ EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, p.7.

⁴⁷ Recital 79 of the draft decision.

⁴⁸ Ibid.

112. As it cannot be ruled out that personal data transferred from the EEA may be processed in Korea for such purposes, the EDPB would also welcome clarifications in the adequacy decision on the existence of the right for a data subject to withdraw consent⁴⁹ and on the right to have his or her personal data erased and no longer processed where the processing is based on consent (such as in case of processing carried out for marketing purposes) and the data subject has withdrawn it.

3.1.13 Automated decision-making and profiling

113. As acknowledged by the European Commission in its draft decision⁵⁰, PIPA and its Enforcement Decree do not contain general provisions addressing the issue of decisions affecting the data subject and based solely on the automated processing of personal data. Still, the Korean legal system envisages such right in the CIA which contains rules on automated decisions (Article 36(2)) even if their application seem to be out of the scope of PIPC supervision (and, as such, out of the scope of application of this draft decision – see section 2.3.2 above on the scope of application of the draft decision).
114. As already considered by the Article 29 Working Party⁵¹ in its opinion 1/2016 on the Privacy Shield and by the EDPB in its previous opinion on the adequacy decision relating to Japan⁵², the growing importance of automated decision-making, profiling and A.I. would suggest taking a more protective approach in this regard. Contrary to the European Commission's arguments⁵³ according to which the absence of specific rules on automated decision-making in the PIPA is unlikely to affect the level of protection as regards personal data that has been collected in the Union (since any decision based on automated processing would typically be taken by the controller in the Union which has a direct relationship with the concerned data subject), the EDPB considers that it cannot be ruled out that automated decision-making could be used by a Korean-based personal information controller in case of data transferred under the adequacy decision (for instance, in the context of employment, for assessing performance at work, reliability, conduct, etc.).
115. Developing new technologies enable companies to more easily implement or consider the implementation of automated decision-making systems which may lead to weakening the position of individuals. Where decisions made solely by those automated systems impact upon the legal situation of individuals or significantly affect them (for example, by black-listing and thereby depriving individuals of their rights) it is crucial to provide for sufficient safeguards including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis⁵⁴.
116. In this context, the EDPB has concerns regarding the lack of legal provisions on automated decision-making in the PIPA and therefore invites the European Commission to address this concern and keep monitoring the development of the Korean legislative framework in this respect.

⁴⁹ See also above under para. 67: While the possibility to revoke consent is clearly envisaged in Article 37(1) CIA, this right is only mentioned twice in PIPA for specific circumstances in Articles 27(1)2 and Article 39(7).

⁵⁰ See Recital 81 of the draft decision.

⁵¹ This Working Party was set up under Article 29 of Directive 95/46/EC. It was an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The WP29 has now become the EDPB.

⁵² Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan adopted on 5 December 2018.

⁵³ Recital 81 of the draft decision.

⁵⁴ WP 254, p. 7.

3.1.14 Accountability

117. The Korean legal framework contains several rules aimed at ensuring that personal information controllers put in place appropriate technical and organisational measures to effectively comply with their data protection obligations and be able to demonstrate such compliance, among other to the competent supervisory authority. In particular, the EDPB welcomes the existence of rules envisaging the adoption of an internal management plan (Article 29 PIPA), the obligation of carrying out a so-called privacy impact assessment (“PIA”) for cases where processing presents a higher risk of possible privacy violations (Article 33(1) PIPA and Article 35 PIPA Enforcement Decree), rules on training and supervision of staff (Article 28 PIPA) as well as the obligation to designate a privacy officer (Article 31 PIPA in conjunction with Article 32 PIPA Enforcement Decree).
118. The EDPB shares the view of the European Commission relating to the essentially equivalent protection they ensure – even in cases where the rules seem to relatively diverge from the ones envisaged by the GDPR, e.g. there is no provision stating the need for the privacy officer to be independent, however, it is clearly set forth that he/she has to report to the management of the personal information controller (Article 31(4) PIPA) and that he/she must not suffer unjustified disadvantages as a consequence of performing these functions (Article 31(5) PIPA) – and would suggest the European Commission monitoring, when reviewing the adequacy decision, the actual application of these provisions in order to assess their effective implementation.

3.2. Procedural and Enforcement Mechanisms

119. Based on the criteria set forth in the GDPR Adequacy Referential, the EDPB has analysed the following aspects of the Korean data protection framework as covered under the draft decision: the existence and effective functioning of an independent supervisory authority; the existence of a system ensuring a good level of compliance and a system of access to appropriate redress mechanisms equipping individuals in the EEA with the means to exercise their rights and seek redress without encountering cumbersome barriers to administrative and judicial redress.
120. In accordance with Chapter VI of the GDPR, and Chapter 3 of the GDPR Adequacy Referential one or more independent supervisory authorities must exist, tasked with monitoring, ensuring, and enforcing compliance with data protection and privacy provisions in a third country to ensure an EEA equivalent level of protection.
121. In this context, the third country supervisory authority must act with complete independence and impartiality in performing its duties and exercising its powers and in doing so shall neither seek nor accept instructions. In addition, the supervisory authority should have all the necessary and available powers and missions to ensure compliance with data protection rights and promote awareness. Consideration should also be given to the staff and budget of the supervisory authority. The supervisory authority shall also be able to start proceedings, on its own initiative.

3.2.1 Competent Independent Supervisory Authority

122. In the Republic of Korea, the independent authority in charge of monitoring and enforcing the PIPA is the PIPC. The PIPC consists of one Chairperson, a Vice Chairperson and seven Commissioners. The Chairperson and Vice Chairperson are appointed by the President upon recommendation of the Prime Minister. Of the Commissioners, two are appointed upon recommendation of the Chairperson, two upon recommendation by representatives from the political party to which the President belongs and the three remaining members upon recommendation by representatives from other political parties (Article 7(2)(2) PIPA). The PIPC is assisted by a Secretariat (Article 7(13)) and may establish sub-commissions (consisting of three Commissioners) to handle minor violations and recurring matters (Article 7(12) PIPA).

123. In this sense, the EDPB acknowledges that despite its recent reorganisation which deeply amended its status and powers, the PIPC has put considerable efforts into building the required infrastructure to accommodate the implementation of the PIPA and its most recent amendments. Among these efforts, reference can be made to the establishment of the PIPC's rules, the elaboration of guidelines to give guidance on the interpretation of the PIPA, and the setting up of a helpline to advise business operators and individuals on data protection provisions as well as a mediation service to handle complaints. In particular, the tasks of the PIPC include advising on laws and regulations related to data protection, developing data protection policies and guidelines, investigating infringements of individual rights, handling complaints, and mediating disputes, enforcing compliance with PIPA, ensuring education and promotion in the area of data protection, and exchanging and cooperating with third country data protection authorities⁵⁵.
124. The appointment and composition of the PIPC are set forth in Article 7(2) PIPA. Although the PIPC falls within the jurisdiction of the Prime Minister (and the Chairperson and Vice Chairperson are appointed by the President upon the recommendation of the Prime Minister), the legal framework mandates that the Commissioners perform their duties independently, according to law and their conscience. The EDPB acknowledges the institutional and procedural safeguards contained in the PIPA and in particular in Articles 7(4) to 7(7). Still, the EDPB would welcome the European Commission to monitor any developments that might affect the independence of the members of the South Korean supervisory authority.
125. Moreover, the draft decision does not yet comprise an analysis of the PIPC's budget, including sources of funding and budget transparency. The EDPB considers that this element, which is mentioned in both, Article 56(1) GDPR and the procedural and enforcement data protection principles and mechanisms to be considered under the GDPR Adequacy Referential when evaluating a country's or an international organization's system, must be thoroughly taken into account as it is an indicator of the economic and human resources available to the supervisory authority to perform its data protection statutory obligations and tasks independently, and would therefore advise the European Commission to account for it in more detail in the draft decision.

3.2.2. Existence of a data protection system ensuring a good level of compliance

126. In the field of enforcement, the EDPB acknowledges the range of enforcement powers and sanctions of the PIPC as provided for in the PIPA and the CIA and takes note of the clarifications contained in Notification No 2021-1 according to which the conditions referred to in Articles 64(1) PIPA and Article 45(4) CIA⁵⁶ will be applicable whenever any of the principles, rights and duties, included in the law to protect personal information, are violated. However, it would recommend the European Commission to closely monitor the application in practice of the PIPC's powers to order the violator to take the measure it deems to be appropriate under the ones listed in Article 64(1) or Article 45(4) CIA.
127. Furthermore, regarding the corrective measures provided in Article 64(1) PIPA, in case of failure to comply with a corrective measure, the PIPC is empowered to impose a fine of a maximum amount of 50 million Korean won (Article 75(2) lit. 13 PIPA). This amount is the equivalent of EUR 36,564. The EDPB considers and has concerns that such limited range of pecuniary sanctions might not have a particularly strong deterrent effect on violators as intended by the law in order to ensure the enforcement of data protection rules since it does not seem appropriately sufficient to dissuade, especially in the case of large organizations or undertakings with significant financial resources.

⁵⁵ The tasks and powers of the PIPC are mainly provided for in Articles 7(8) and 7(9), as well as in Articles 61 to 66 PIPA.

⁵⁶ I.e., "*a violation of the law is deemed to be likely to infringe on the rights and freedom of individuals in regard to personal information and failure to take action is likely to cause damage that is difficult to remedy*".

128. With respect to the possibility that the PIPC may demand that the head of a central administrative agency investigates the personal information controller or jointly engages in an investigation into violations of PIPA and even impose corrective measures with respect to personal information controllers under their jurisdiction (Article 63(4)-(5) PIPA), the EDPB notes that, even though some information has been provided in Recital 122 of the draft decision, overall the nature of these other agencies and their legal relations with the PIPC remains rather unclear. Additionally, Article 68(1) PIPA refers to many entities to which it would be possible to delegate the authority of the PIPC. Even if it seems that this provision has been applied only in relation to the Korean Internet and Security Agency⁵⁷, the EDPB would welcome clarifications with regards to the nature of the possible interactions between these entities and an attentive monitoring of the application of this provision in the future in order to ensure the independence of the entities tasked with applying the data protection rules.
129. With regard to sanctions, the Korean system seems to combine different types of sanctions, from corrective measures and administrative fines to criminal sanctions, which are likely to have a strong deterrent effect, and the Korean authorities presented several examples of fines imposed recently by the PIPC, *inter alia* one of 6.7 billion Korean won imposed in December 2020 on a company for violating different provisions of PIPA, and another fine of 103.3 million Korean won on 28 April 2021 issued to an AI Technology company for violating the rules of lawfulness of processing, in particular consent, and the processing of pseudonymised information.
130. Although the above-mentioned amounts may have a dissuasive effect, the EDPB would welcome additional information on the method used by the PIPC to calculate the level of administrative fines, for example with respect to fines imposed for a failure to comply with a corrective measure issued pursuant to Article 64(1) PIPA (see Article 75(2) lit. 13 PIPA). This is especially relevant concerning criminal sanctions and the application of the (Korean) Criminal Act.

3.2.3. The data protection system must provide support and help to data subjects in the exercise of their rights and appropriate redress mechanisms

131. Concerning redress, the Korean system seems to offer various avenues to ensure adequate protection and, in particular, the enforcement of individual rights with an effective administrative and judicial redress, including compensation for damages.
132. The Korean system also offers alternative mechanisms to which individuals can turn to obtain redress, in addition to administrative and judicial avenues, as explained in Recitals 132 and 133 of the draft decision, relating to the Privacy Call Centre and the Dispute Mediation Committee respectively. As these are additional redress avenues, the EDPB would welcome more detailed explanations on how they complement the redress possibilities before the PIPC and courts for the data subjects whose personal data is transferred to Korea under the adequacy decision.

4. ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN SOUTH KOREA

133. With regard to the assessment of the level of data protection in the areas of law enforcement and national security, the European Commission provided comprehensive information in its draft decision and the annexes made available. Therefore, the EDPB refrains from reproducing most of the factual findings and assessments in this opinion.

⁵⁷ See Recital 117 of the draft decision and Article 62 Enforcement Decree.

- 134. The European Commission comes to the conclusion that in the above-mentioned areas a level of data protection exists that corresponds to the requirements set by the case law of the CJEU and can therefore be considered essentially equivalent to that of the European Union.
- 135. As a general remark, the EDPB would like to emphasize that even in cases where it seems or is claimed by the European Commission that data transferred from the EU to South Korea is unlikely to be affected by the relevant Korean law, it is still in order to assess the adequacy of the Korean level of data protection with regard to such cases. Their relevance is also demonstrated by the fact that the European Commission itself has addressed them in the draft decision.

4.1 General data protection framework in the context of government access

- 136. When it comes to access to personal data by public authorities, various Korean laws have to be looked at in order to assess the level of protection of the right to privacy and data protection. First of all, the EDPB notes that PIPA, as a key data protection law, claims broad applicability. However, while PIPA is fully applicable to the area of law enforcement, its application to data processing for national security purposes is limited. Pursuant to Article 58(1) lit.2 PIPA, Chapters III through VII do not apply to the processing of personal data for national security purposes. Yet, Chapters I, II, IX and X remain applicable for the area of national security. Thus, PIPA's core principles as well as the fundamental guarantees for data subject rights and the provisions on supervision, enforcement and remedies do apply to the access and use of personal data by national security authorities.
- 137. The South Korean constitution too enshrines essential data protection principles, namely the principles of legality, necessity and proportionality. These principles are also applicable to the access to personal data by South Korean public authorities in the areas of law enforcement and national security⁵⁸.
- 138. In the area of law enforcement the police, prosecutors, courts and other public bodies may collect personal data based on specific legislation, i.e. the Criminal Procedure Act ("CPA"), the Communications Privacy Protection Act ("CPPA"), the Telecommunications Business Act ("TBA") and the Act on Reporting and Using Specified Financial Transaction Information ("ARUSFTI"), which applies to the prosecution and prevention of money laundering and terrorist financing. These particular laws set out further limitations, safeguards and exemptions.
- 139. In the area of national security, based on the National Intelligence Service Act ("NISA") and further "national security laws"⁵⁹, the National Intelligence Service ("NIS") may collect personal data and intercept communications. In conducting its powers the EDPB understands that the NIS has to comply with the aforementioned legal provisions as well as with PIPA.
- 140. The EDPB asks the Commission to clarify whether there are other authorities in Korea besides the NIS that are responsible for the area of national security as in Annex I, Section 6 the European Commission gives the impression of the NIS as an example for national security agencies.

4.2 Protection and safeguards for communication confirmation data in the context of government access for law enforcement purposes

- 141. On the basis of the relevant law, the CPPA, law enforcement authorities may take two types of measures for access to communication information. The CPPA distinguishes between communication-restricting measures, which cover both the collection of the content of ordinary mail and the direct

⁵⁸ See Recital 145 of the draft decision.

⁵⁹ National security laws include, for instance, the Communications Privacy Protection Act, the Act on Anti-Terrorism for the Protection of Citizens and Public Security or the Telecommunications Business Act.

interception of the content of telecommunications⁶⁰, and the collection of so-called communication confirmation data. The latter include the date of telecommunications, their start- and end-time, the number of outgoing and incoming calls as well as the subscriber number of the other party, the frequency of use, log files on the use of telecommunication services and location information⁶¹.

142. The EDPB notes that communication confirmation data seem not to benefit from the same safeguards as data collected via communication-restricting measures, i.e. content data. Indeed, the EDPB notices that the collection of content benefits from more safeguards than the collection of communication confirmation data for law enforcement purposes: First, unlike the collection of content data, the collection of communication confirmation data is not limited to the investigation of certain serious crimes, but can be performed when deemed necessary to conduct “any investigation or to execute any punishment” (Article 13(1) CCPA). Second, the collection of communication confirmation data is in principle not structured as a measure of last resort and only to be used where it is difficult to otherwise prevent the commission of a crime, arrest the criminal or collect evidence⁶². Communication confirmation data can be collected whenever a prosecutor or judicial police officer “deems it necessary” for investigating a crime or executing a punishment. However, an exception exists in this regard for real-time tracking data and communication confirmation data concerning a specific base station according to Article 13(2) CCPA. Third, law enforcement agencies collecting the content of communication must immediately cease to do so once continued access is no longer deemed to be necessary⁶³. With regard to communication confirmation data, this is at least not explicitly stipulated in the CCPA or its Enforcement Decree.
143. The EDPB takes note that the collection of communication confirmation data may only take place on the basis of a court-issued warrant. Moreover, the CCPA requires detailed information to be provided both in the application for the warrant and in the warrant itself⁶⁴. Such prior judicial authorisation serves to limit the law enforcement authorities’ discretion in applying the law and to verify whether sufficient reasons for collecting communication confirmation data exist in each case. The EDPB also recognises that the law of the Republic of Korea does not seem to provide for general and indiscriminate retention of communication confirmation data. Thus, government access to such data always relates to data that is still retained for the purposes of billing and providing the communication services themselves.
144. However, the EDPB stresses that the CJEU has questioned the fact that traffic data are less sensitive than others, and in particular than content data⁶⁵. Taking into account that communication confirmation data is afforded a lower level of protection than content data in several respects, the EDPB invites the European Commission to closely monitor whether the safeguards provided under Korean law for such category of personal data ensure an essentially equivalent level of protection to

⁶⁰ Articles, 3(2), 2(6), 2(7)CCPA.

⁶¹ Article 2(11) CCPA.

⁶² This is the case for content data according to Articles 3(2) and 5(1) CCPA.

⁶³ Article 2 CCPA Enforcement Decree.

⁶⁴ See Recital 156 of the draft decision.

⁶⁵ See CJEU, C-623/17, *Privacy International*, 6 October 2020, ECLI:EU:C:2020:790, para. 71: “*The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications. In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance (see, by analogy, judgments of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238, paragraphs 27 and 37, and of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraphs 99 and 100).*”

the one guaranteed in the EU, in particular with regard to proportionality and foreseeability of the law.

4.3 Access to communication information by Korean public authorities for national security purposes

145. With regard to the legal framework for access of national security authorities to communication information transferred from the EEA to Korea, the EDPB has identified two points of concern, both of which relate to the regime of access to communications between non-Korean nationals that fall within a specific set of use cases (see paragraph 29). In those cases, with respect to both communication confirmation data and content data, certain safeguards otherwise provided are not applicable. In other words, in these specific cases, these data do not benefit from the same safeguards as data communicated when at least one Korean national is involved in the communication.

4.3.1 No obligation to notify individuals of government access to communications between foreign nationals

146. In a scenario as outlined above, i.e. where none of the parties of a communication is a Korean national, national security authorities are not obliged to notify individuals about the collection and processing of their data. The EDPB recognises that this issue affects only certain cases. Firstly, as already pointed out, whenever at least one Korean national is involved in a communication, the notification requirements according to the CCPA apply to all parties of the communication irrespective of their nationality⁶⁶. Secondly, the collection of personal data stemming from communications exclusively between foreign nationals is subject to a specific set of use cases. In particular, the right to access in such cases extends to communications of a) countries hostile to the Republic of Korea, b) foreign agencies, groups or nationals suspected of engaging in anti-Korean activities⁶⁷, or c) members of groups operating within the Korean Peninsula but effectively beyond the sovereignty of the Republic of Korea and their umbrella groups based in foreign countries. Communications between EU individuals transferred from the EEA to Korea can thus only be collected for national security purposes if they fall within one of the three above-mentioned categories⁶⁸. As a further limiting factor, the EDPB understood from the additional explanations of the European Commission that the applicable legal framework does not provide for the interception of data in transit outside of Korea.
147. Hence, the criticality of the lack of a notification requirement might, in terms of its practical impacts, be considered as limited. However, the EDPB stresses the importance of the (subsequent) notification of government access, in particular with regard to ensuring effective remedies. According to the CJEU, notification is “*necessary to enable the persons affected to exercise their rights under Articles 7 and 8 of the Charter to request access to their personal data that has been the subject of those measures and, where appropriate, to have the latter rectified or erased, as well as to avail themselves, in accordance with the first paragraph of Article 47 of the Charter, of an effective remedy before a tribunal*”⁶⁹. Government access for purposes of national security oftentimes includes secret surveillance measures, meaning that the objects of the surveillance, the data subjects, are not aware of the processing of their data. Thus, there “*is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his knowledge and thus able to challenge their legality retrospectively or, in the alternative, unless any person who suspects*

⁶⁶ See Recital 192 of the draft decision.

⁶⁷ See Annex II, footnote 244, according to which the notion of anti-Korean activities refers to activities that threaten the nation’s existence and safety, democratic order or the people’s survival and freedom.

⁶⁸ See Recital 187 of the draft decision.

⁶⁹ CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, ECLI:EU:C:2020:791, para. 190.

*that his communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications*⁷⁰. In this context and consistent herewith, the EDPB has many times expressed its concern with effective remedies in surveillance cases. The EDPB emphasises that the secrecy of government measures must not result in such measures being effectively unchallengeable. Against this background, whether or not the lack of a notification requirement for communications between foreign nationals impacts the level of data protection as assessed in the draft decision has to be evaluated as part of an overall assessment with special regard to the oversight and redress mechanisms provided under Korean law (see sections 4.7 and 4.8).

148. In addition, the EDPB notes in this context that the law refers to rather broad terms such as anti-Korean or antinational activities⁷¹ and that it is difficult to foresee how these concepts are construed under Korean law. The EDPB invites the European Commission to monitor how these terms are fleshed out in Korean law and whether their application in practice meets the requirements of proportionality following from EU law.

4.3.2 No prior independent authorisation for collection of communication information between foreign nationals

149. In cases where EEA personal data derived from communications between non-Korean nationals (and falling within one of the abovementioned use cases) are to be processed in Korea for national security purposes, the collection of such data is not subject to prior approval by an independent body (as is the case for communications where at least one of the individuals concerned is a Korean national).⁷²
150. Especially in light of the recent decisions of the European Court of Human Rights (“ECtHR”) “Big Brother Watch and Others v. UK” and “Centrum för Rättvisa v. Sweden”, the EDPB considers it necessary to explore whether this constitutes a critical shortcoming of the Korean data protection framework. In this regard, the EDPB recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures,⁷³ Article 6(3) of the Treaty on the European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law while, as the CJEU recalls in its jurisprudence, the latter does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law⁷⁴. Thus, the level of protection of fundamental rights required by Article 45 of the GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the Charter. This being said, according to Article 52(3) of the Charter the rights contained therein which correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by that Convention. Consequently, the jurisprudence of the ECtHR concerning rights that are also foreseen in the Charter must be taken into account, as a

⁷⁰ ECtHR, *Big Brother Watch and others v. UK*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, para. 337 and ECtHR, *Case of Roman Zakharov v. Russia*, 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306, para. 234.

⁷¹ The European Commission has explained that, according to explanations from the Korean government, this refers to ‘activities that threaten the nation’s existence and safety, democratic order or the people’s survival and freedom’, see also footnote 319 of the draft adequacy decision.

⁷² See Recital 190 of the draft decision.

⁷³ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, paras. 10, 11.

⁷⁴ See CJEU, C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems*, 16 July 2020, ECLI:EU:C:2020:559 (hereinafter “Schrems II”), para. 98.

minimum threshold of protection to interpret corresponding rights in the Charter, i.e. to the extent that the Charter, as interpreted by the CJEU, does not provide for a higher level of protection⁷⁵.

151. The EDPB notes that, while prior (independent) approval of surveillance measures is deemed an important safeguard against arbitrariness, such approval cannot be derived from the jurisprudence of the CJEU as an absolute requirement for the proportionality of surveillance measures. However, the ECtHR has now explicitly established the requirement of ex ante independent authorisation for bulk interception⁷⁶. While the draft decision does not explicitly say so, the EDPB understands that the legal framework of the Republic of Korea does not provide for bulk interception but only for targeted interception of telecommunications⁷⁷. The European Commission has confirmed this understanding.
152. That being said, the above-mentioned decisions of the ECtHR, in line with the case law of the CJEU⁷⁸ and previous case law of the ECtHR⁷⁹, once again show the importance of comprehensive supervision by independent supervisory authorities. The EDPB emphasizes that independent oversight at all stages of the process of government access for law enforcement and national security purposes is an important safeguard against arbitrary surveillance measures and thus for the assessment of an adequate level of data protection. The guarantee of independence of the supervisory authorities within the meaning of Article 8(3) of the Charter is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals with regard to the processing of personal data. This applies in particular in circumstances where, due to the nature of secret surveillance, the individual is prevented from seeking review or from taking a direct part in any review proceedings prior or during the execution of the surveillance measure.
153. The lack of prior independent approval cannot in itself be considered as a substantial shortcoming in Korean law with respect to the assessment of an essentially equivalent level of data protection. The assessment of adequacy depends, again, on all the circumstances of the case, in particular on the effectiveness of ex post oversight and legal redress as provided for in the legal framework of Korea (see further sections 4.7 and 4.8).

4.4 Voluntary disclosures

154. According to Article 83(3) TBA, telecommunication service providers may voluntarily hand over so-called “subscriber data”⁸⁰ to national security and law enforcement authorities upon request. While the EDPB notes that cases involving personal data that have been transferred from the EEA to Korea are likely to be rare, they still need to be analysed in order to assess the level of data protection, as already mentioned above.

⁷⁵ See CJEU, joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others*, 6 October 2020, para. 124.

⁷⁶ See ECtHR, *Big Brother Watch and others v. UK*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, para. 351: “Bulk interception should be subject to independent authorization at the outset”, “bulk interception should be authorized by an independent body; that is, a body which is independent of the executive”.

⁷⁷ Only Annex II, section 3.2 contains an explicit declaration for national security purposes when it is specified that the limitations and safeguards “ensure that the collection and processing of information is limited to what is strictly necessary to achieve a legitimate objective. This excludes any mass and indiscriminate collection of personal information for national security purposes”.

⁷⁸ See, for example, CJEU joined cases C-203/15 and C-698/15, *Tele2 Sverige AB and others*, ECLI:EU:C:2016:970.

⁷⁹ See, for example, ECtHR, *Case of Roman Zakharov v. Russia*, 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

⁸⁰ Concerned datasets would be: the name, resident registration number, address and phone number of users, the dates on which users subscribe or terminate their subscription as well as user identification codes (used to identify the rightful user of computer systems or communication networks).

155. The EDPB understands that in these cases the data protection safeguards of PIPA apply and public authorities, as well as telecommunications providers, have to comply with these requirements⁸¹ and that both can be held liable for any infringement of the rights and freedoms of the concerned data subjects⁸². Furthermore the EDPB understands that telecommunications providers are not required to comply with such requests.
156. However, with regard to the concept of access to subscriber data by national authorities for law enforcement as well as and in particular for national security purposes via “voluntary disclosure” of telecommunication business operators, there is a concern of increased risk to the rights and freedoms of data subjects, especially with regard to their right to information.
157. According to Article 58(1) lit.2 PIPA, the provisions of Chapter III through VII shall not apply to any personal information requested to be provided related to national security. In this respect, for example, the provisions of Article 18 (Limitation to Out-of-Purpose Use and Provision of Personal Information) and Article 20 (Notification on Sources, etc. of Personal Information Collected from Third Parties) of PIPA are not applicable to such requests. In cases where a request is made by a national security authority, this raises the question, on the one hand, of whether Article 58(1) lit. 2 also precludes the application of PIPA to telecommunications providers as well. On the other hand, the question arises whether the exclusion of the application of Article 20 PIPA in such cases also applies to the corresponding provision from Section 3 of Annex I (Notification for the data where personal data have not been obtained from the data subject (Article 20 of the Act)). If this were the case and if Article 58(1) lit. 2 also addressed telecommunications providers, there would be a risk, according to the available information, that there would be no legal obligation to inform the data subjects about the voluntary disclose.
158. The EDPB is therefore concerned about the effectiveness that the information requirements could be rendered ineffective, making it considerably more difficult for data subjects to assert their data protection rights especially with regard to judicial redress. In this respect, the EDPB invites the European Commission to clarify the scope of the relevant provisions.

[4.5 Further use of information](#)

159. The principle of purpose limitation is a core legal requirement of data protection. It requires that personal data is only to be collected for specified, explicit and legitimate purposes and not to be further processed in an incompatible way to those purposes. Furthermore public authorities are under EU law permitted to process personal data for the prevention, investigation or prosecution of criminal offenses even if those data were initially obtained for different purpose if these authorities have a legal basis to process such data under the relevant law and if the further processing is not disproportionate⁸³.
160. According to this the EDPB notes that the Korean data protection framework provides for similar safeguards and limitations to the ones provided under EU law in relation to the further use of the information collected for law enforcement and national security purposes, e.g. Article 3(1)-(2) PIPA principle of purpose limitation.

[4.6 Onward transfers and intelligence sharing](#)

161. Article 44 GDPR provides that transfers and onward transfers of personal data shall only take place if the level of protection guaranteed by the GDPR is not undermined. Thus, the level of protection afforded to personal data transferred from the EEA to Korea must not be undermined by the further

⁸¹ See Recitals 164 and 194 of the draft decision.

⁸² See Recital 166 of the draft decision.

⁸³ See Article 4(2) LED.

transfer to recipients in a third country, i.e. onward transfers should be permitted only where a continued level of protection essentially equivalent to the one provided under EU law is ensured. Consequently, when assessing whether a third country ensures an adequate level of data protection, the country's legal framework for onward transfers must be taken into account. This is undisputed and in line with the view of both the European Commission⁸⁴ and the EDPB.

162. In this context, the EDPB takes note that the ECtHR has in its recent decisions "Big Brother Watch and Others v. UK" and "Centrum för Rättvisa v. Sweden" provided guidance⁸⁵ regarding the data protection precautions to be observed in Contracting States when communicating personal data to other parties for law enforcement and national security purposes in bulk collection cases: "*First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. [...] Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred.*"⁸⁶
163. In applying these standards, the ECtHR found in "Centrum för Rättvisa v. Sweden" that the absence of any express legal requirement in the interception regime to assess the necessity and proportionality of intelligence sharing for its possible impact on the right to privacy constitutes a violation of Article 8 ECHR. The ECtHR criticised that, as a result of the level of generality of the law, intercept material could generally be sent abroad whenever this is considered to be in the national interest irrespective of whether the foreign recipient offers an acceptable minimum level of safeguards⁸⁷.
164. Acknowledging that the legal framework of South Korea does not allow for bulk interception, still in light of the implications of the jurisprudence of the ECtHR as outlined above, the EDPB considers that, in addition to the requirements stemming from EU law as interpreted by the CJEU, the ECtHR's line of arguments should be considered for assessing whether the legal framework for onward transfers to a third country provides for adequate data protection standards.

4.6.1 Applicable legal framework for onward transfers by law enforcement authorities

165. In regard to onward transfers by the competent authorities for law enforcement purposes, the EDPB understands from the explanations by the European Commission that the Section 2 of Annex I of the draft decision concerning the limitation of onward transfers is applicable, including when the transfer is made on the basis of a statute other than PIPA. According to this rule, "*if personal information is provided to a third party overseas, it may not receive the level of protection guaranteed by the Personal Information Protection Act of Korea due to differences in personal information protection systems of different countries. Accordingly, such cases will be deemed as 'cases where disadvantages may be caused to the data subject' mentioned in Paragraph 4 of Article 17 of the Act or 'cases where the interest of a data subject or third party is infringed unfairly' mentioned in Paragraph 2 of Article 18 of the Act and Article 14(2) of the Enforcement Decree of the same Act. To fulfil the requirements of these provisions, the personal information controller and third party must therefore explicitly ensure a level of protection equivalent to the Act, including the guarantee of the data subject's exercise of his/her*

⁸⁴ See Recital 84 et seq. of the draft decision.

⁸⁵ The following elements were established on the occasion of the cases *Big Brother Watch* and *Centrum för Rättvisa*, which concern bulk interception regimes. The requirement of precautions to be taken when communicating material to other parties was already part of the criteria developed by the ECtHR in the context of targeted interception and had not been further specified by the ECtHR (see *Big Brother Watch and Others v. UK*, para. 335, 362).

⁸⁶ ECtHR, *Big Brother Watch and others v. UK*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD005817013, para. 362.

⁸⁷ See ECtHR, *Centrum för Rättvisa v. Sweden*, 25 May 2021, ECLI:CE:ECHR:2021:0525JUD003525208, para. 326.

*rights in legally binding documents such as contracts, even after personal information is transferred overseas*⁸⁸.

166. The EDPB welcomes this provision, which, assuming the adequacy of the level of data protection in Korea for this purpose, ensures the continuity of a level of protection as essentially afforded under EU law for onward transfers. The Commission has confirmed that the EDPB's understanding, namely that this section of Annex I applies to all onward transfers by the competent authorities for law enforcement purposes, is correct. However, the EDPB points out that it must be ensured that this regulation provides for a continued level of protection in practice as there may be uncertainty as to which contractual safeguards and obligations or other similar mechanisms can be used to achieve such a level of protection in case of processing for law enforcement purposes. In this regard, it should be additionally stated, for example, that personal data may only be shared with the relevant competent authorities in the third country.
167. Subject to the clarification requested above as to whether KOFIU is covered by the draft decision the EDPB notes that the official representation on government access⁸⁹ explains that, according to Article 8(1) of the ARUSFTI, the Commissioner of the KOFIU may provide foreign financial intelligence services with specified financial transaction information, if deemed necessary to achieve the purpose of the ARUSFTI⁹⁰. Article 8 ARUSFTI itself does not provide for an obligation to determine whether and ensure that the foreign country offers adequate data protection safeguards. Annex II does not refer to the new section of Annex I in this regard. Therefore, the EDPB calls on the European Commission to clarify the interrelation of the relevant section of Annex I on the limitation of onward transfers and the legal basis for onward transfers according to the ARUSFTI.

4.6.2 Applicable legal framework for onward transfers for national security purposes

168. The draft decision does not contain any information on the legal framework for onward transfers in the field of national security. To this end, the EDPB understands that, unlike for law enforcement purposes, the Section 2 of Annex I is not applicable to onward transfers for national security purposes. Articles 17 and 18 of PIPA which are subject of the Annex I section in question are part of Chapter III of PIPA which in turn is not applicable to the processing of personal data for national security purposes (Article 58(1) PIPA).
169. However, the EDPB assumes that Korea may need to and does transmit personal data to foreign intelligence services for national security purposes, e.g. in order to cooperate on combatting cross-border threats to national security, to warn foreign governments about or to solicit their help in identifying such threats.
170. The EDPB understood that, in the view of the European Commission, onward transfers are sufficiently regulated in Korean law by the safeguards following from the overarching constitutional framework, in particular the principles of necessity and proportionality, as well as by the core data protection principles regulated in PIPA, such as lawfulness and fairness of processing, purpose limitation, data minimisation, security and the general obligations to prevent abuse and misuse of personal information.
171. The EDPB recognises and acknowledges the general applicability of these key (data protection) principles but raises concerns that these safeguards are being of a very general nature and do not

⁸⁸ Draft decision, Annex I, p. 7.

⁸⁹ See draft decision, Annex II.

⁹⁰ See draft decision, Annex II, section 2.2.3.2. While such an exchange may only take place subject to the condition that the foreign service may not use the information for any purpose other than the original purpose of disclosure, and in particular not for a criminal investigation or trial (Article 8(2) ARUSFTI), the Commissioner of the KOFIU may, in receipt of a request by a foreign country, give consent to the use of such data for criminal investigations or trials for criminal offenses with a prior consent of the Minister of Justice (Article 8(3) ARUSFTI).

specifically refer to or address, in a legal basis, the specific circumstances and conditions for onward transfers of EEA transferred data for national security purposes. While these general and overarching principles are broadly applicable, the EDPB questions whether this could be considered to meet the criteria of clear and precise rules and to sufficiently enshrine effective and enforceable safeguards. Especially where government access and processing of personal data is exercised in secret and the inferences that could be drawn from the data are particularly severe, it is essential to have clear, detailed rules. The law should indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection. In the *Schrems II* ruling, the CJEU recalls that a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principles of necessity and proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and impose minimum safeguards⁹¹. The EDPB is therefore concerned that it is not sufficient that such safeguards are generally enshrined in higher-ranking law without specifically implementing the notion of e.g. proportionality in the respective legal basis itself.

172. These concerns are supported by the above-mentioned decision of the ECtHR, in which the court found that a general rule without any express requirement to assess necessity and proportionality or consider privacy concerns is not compatible with the right to privacy pursuant to Article 8 ECHR. In this regard, the EDPB notes that in the law of the case at stake (as well as in the law of Korea) overarching (constitutionally guaranteed) principles of necessity and proportionality do exist, e.g. according to the Charter and through the accession to the ECHR.
173. The EDPB invites the European Commission to clarify the legal basis, how and to what extent and under which specific conditions intelligence service agencies are obliged to consider privacy concerns and data protection safeguards prior to disclosing personal data for national security purposes to foreign partners. In case such obligation is derived directly from constitutional principles, the European Commission should further assess the requirements of preciseness and clarity of the relevant law and confirm that the general constitutional and data protection principles are appropriately applied and implemented.

4.6.3 International agreements

174. The EDPB notes that the European Commission did not consider, as part of its adequacy assessment, the existence of international agreements concluded between Korea and third countries or international organisations that may provide for specific provisions for the international transfer of personal data by law enforcement and/or intelligence services to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of law enforcement or intelligence cooperation are likely to affect the data protection legal framework of Korea as assessed.
175. The EDPB therefore invites the European Commission to clarify whether such agreements exist, under which conditions they may be concluded and assess whether the provisions of international agreements may affect the level of protection afforded to personal data transferred from the EEA to Korea by the legislative framework and practices in relation to overseas disclosures for law enforcement and national security purposes.

4.7 Oversight

176. The EDPB notes that the oversight of criminal law enforcement as well as national security authorities is ensured by a combination of different internal and external bodies.

⁹¹ See *Schrems II*, paras. 175 and 180.

177. In this context, it is to be noted that the CJEU has repeatedly stressed the need for independent oversight as an essential component of the protection of natural persons with regard to the processing of their personal data. The concept of independence encompasses the areas of institutional autonomy, freedom from instructions and material independence. In order to ensure a consistent monitoring and enforcement of data protection law, supervisory authorities must have effective powers, including corrective and remedial powers.
178. The EDPB agrees with the conclusion of the European Commission that, in an overall assessment, Korea can be considered to have an independent and effective supervisory system even though several bodies of the supervisory system do not meet the above requirements in themselves. For example, most of them do not have executive powers, but are limited to mere recommendations, e.g. the National Human Rights Commission or the Board of Audits and Inspections. Furthermore, most of the respective public bodies are not exclusively data protection institutions, but are usually entrusted with other tasks in the area of fundamental rights protection.
179. However, according to the European Commission's explanations, the EDPB notes that the supervision of law enforcement authorities is comprehensively and without exception guaranteed by the PIPC. Therefore the PIPC possesses investigative, remedial and enforcement powers under PIPA and other data protection laws (e.g. the CCPA) which apply to the entire area of access to personal data by law enforcement and national security authorities.
180. In this context, the EDPB would like to emphasize once again that in order to exercise their tasks and powers, supervisory authorities need to be equipped with sufficient human, technical and financial resources. In this regard, there is unfortunately a lack of any information on the designated supervisory bodies, in particular the PIPC. Therefore, the EDPB repeats its request to the European Commission to provide further information on the matter.
181. Overall, the EDPB would like to note that there are hardly any statements, examples or figures in the draft decision regarding the supervisory activities as well as the legal enforcement of data protection law by the supervisory bodies in the area of law enforcement and national security. These would be helpful in the context of evaluating the effectiveness of the supervisory bodies.

4.8 Judicial remedy and redress

182. The EDPB recalls that it is essential for an adequate level of data protection that data subjects are provided with comprehensive remedies and redress against unauthorized data access or processing. These legal remedies must be sufficient to enable the data subject to obtain access to the data stored about him or her and to request that it be corrected or deleted.
183. In the light of the *Schrems I* and *Schrems II* judgments by the CJEU, it is clear that in addition to the right to turn to competent authorities, effective judicial protection in the meaning of Article 47(1) of the Charter is of fundamental importance for the assumption of adequacy of the law of a third country.
184. The EDPB recognises that Korea has established various avenues for the execution of individuals' rights of access, retention, deletion and suspension under PIPA. Those rights can be executed towards the controller itself or via a complaint lodged with the PIPC or other supervisory bodies, e.g. the National Human Rights Commission. Furthermore, the EDPB recognises the possibility to challenge controllers or public authorities' decision in response to their request on the basis of the Administrative Litigation Act.
185. In addition, The EDPB understands from the explanations given by the European Commission that individuals may challenge the actions of law enforcement and national security authorities before

competent courts under the Administrative Litigation Act and Constitutional Court Act, and have the possibility to obtain compensation for damages under the State Compensation Act⁹².

186. In this context, however, the EDPB is concerned about effective redress for EU individuals in national security cases where no Korean citizen is involved. As noted in paragraph 33 et seq., national security authorities are not required to notify data subjects of the collection and processing of their personal data. Since it is considerably more difficult to obtain effective legal protection in these cases, the EDPB would like to point out that certain legal safeguards are required here if data transferred from the EEA is involved. These safeguards must enable data subjects to take effective action against unlawful data processing in a legally secure manner without being hindered by excessively narrow procedural requirements, e.g., by the imposition of a burden of proof that they cannot meet without knowledge of the processing. Furthermore, data subjects have to be able to turn to a competent body that meets the requirements of Article 47 CFR, i.e. which is competent to determine that a data processing is taking place, to verify the lawfulness of the processing, and to have enforceable remedial powers in the event the data processing is unlawful. Against this background, a mere right of complaint to the NHRC, for example, would not be sufficient. The EDPB therefore calls on the Commission to explain in more detail how these requirements are implemented in procedural and substantive terms, e.g., whether it is possible for data subjects to turn to the PIPC as well as to a court without having to prove the data processing in question.
187. In addition, the EDPB observes that the draft decision foresees a complaint referral mechanism, i.e. that EU individuals may submit a complaint to the PIPC through their national data protection authority or the EDPB. The PIPC will then notify the individual via the same channel once the investigation is concluded⁹³. The EDPB welcomes the effort to facilitate easier access to redress against Korean national security authorities. At the same time, the EDPB advocates that such a referral mechanism is channelled through the European national data protection authorities rather than through the EDPB as they are competent and closer to the handling of the individual complaints.
188. Furthermore, the EDPB notes a possible contradiction with respect to voluntary disclosures. On the one hand, the draft decision states that individuals are able to obtain redress in case their data is disclosed unlawfully following a request for voluntary disclosure, including against the law enforcement authority issuing the request⁹⁴. On the other hand, the draft decision makes reference to the requirement of direct impact regarding the individual's right to challenge the actions of public authorities, listing (only) binding disclosure requests as an example for a case where administrative action is considered to directly impact on the right to privacy⁹⁵. The EDPB understands from explanations from the European Commission that there is actually no restriction of the redress possibilities against requests for voluntary disclosure and therefore asks the European Commission to further clarify this in the decision, both in the areas of law enforcement and national security (unlike the section on law enforcement, the section on voluntary disclosures for national security purposes does not contain any explicit statement on redress in this context).

⁹² See Annex II, 3.2.4 in conjunction with 2.4.3.

⁹³ See Recital 205 and Annex I, p. 19 of the draft decision.

⁹⁴ See Recital 166 of the draft decision.

⁹⁵ See Recital 181 (law enforcement) and Recitals 208 and 181 (national security) of the draft decision.

Opinion of the Board (Art. 70.1.s)



**Opinion 5/2023 on the European Commission Draft
Implementing Decision on the adequate protection of
personal data under the EU-US Data Privacy Framework**

Adopted on 28 February 2023

Executive summary

On 13 December 2022, the European Commission published a draft adequacy decision ('Draft Decision') which includes annexes constituting a new framework for transatlantic exchanges of personal data, the EU-U.S. Data Privacy Framework ('DPF'), which is meant to replace the previous U.S. Privacy Shield invalidated by the Court of Justice of the European Union ('CJEU') on 16 July 2020, in the Schrems II case. The key component of the DPF is the EU-US Data Privacy Framework Principles, including the Supplemental Principles (collectively 'the DPF Principles').

In accordance with Article 70(1)(s) of Regulation (EU) 2016/679¹ of the European Parliament and of the Council ('GDPR'), the Commission requested the opinion of the European Data Protection Board ('EDPB') on the Draft Decision.

The EDPB assessed the adequacy of the level of protection afforded in the USA, on the basis of the examination of the Draft Decision. The EDPB assessed both the commercial aspects and the access to and use of personal data transferred from the EU by public authorities in the US.

The EDPB took into account the applicable EU data protection legal framework as set out in the GDPR, as well as the fundamental rights to private life and data protection as enshrined in Articles 7 and 8 of the Charter of Fundamental rights of the European Union and Article 8 of the European Convention on Human Rights. It also considered the right to an effective remedy and to a fair trial laid down in Article 47 of the Charter, as well as the jurisprudence related to the various fundamental rights.

In addition, the EDPB has considered the requirements of the Adequacy Referential adopted by the EDPB².

The EDPB's key objective is to give an opinion to the Commission on the adequacy of the level of protection afforded to individuals whose personal data is transferred to the US. It is important to recognise that the EDPB does not expect the US data protection framework to replicate European data protection law.

However, the EDPB recalls that, to be considered as providing an adequate level of protection, Article 45 GDPR and the case-law of the CJEU require the third country's legislation to provide data subjects with a level of protection essentially equivalent to that guaranteed in the EU.

1.1. General data protection aspects

The DPF provides that adherence to the DPF Principles by DPF Organisations may be limited in some cases (e.g. to the extent necessary to comply with a court order or to meet public interest). In order to better identify the impact of these exemptions on the level of protection for data subjects, the EDPB recommends that the Commission includes in the Draft Decision clarification on the scope of the exemptions, including on the applicable safeguards under US law.

The EDPB notes that the structure of the annexes and their numbering makes the information rather difficult to find and refer to. This contributes to an overall complex presentation of the new framework,

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88.

² Art. 29 Working Party, Adequacy Referential, WP 254 rev.01, 28 November 2017, as last revised and adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018 (hereinafter 'Adequacy Referential').

which compiles in its annexes documents of different legal value, and may not favour a good understanding of the DPF Principles by data subjects, DPF Organisations, and EU Data Protection Authorities. The EDPB also stresses that the terminology should be used consistently throughout the DPF. Similarly, the definition of some essential terms is lacking³.

The EDPB welcomes the updates made to the DPF Principles⁴, which will constitute the binding legal framework for DPF Organisations, but notes that despite a number of changes and additional explanations made in the recitals of the Draft Decision, the DPF Principles to which the DPF organisations have to adhere remain essentially unchanged with regard to those applicable under the Privacy Shield (on which were based the Working Party 29 ('WP29') and EDPB annual joint reviews). The DPF Principles are also, to a large extent, the same as those of the draft Privacy Shield on which the WP29 based its 2016 opinion⁵. For those DPF Principles that are substantially unchanged, the EDPB considers not necessary to repeat all comments previously made by the WP29. The EDPB has decided to focus on specific aspects that it considers to be even more relevant today, in view of the evolution of the legal and technological environment.

For instance, the EDPB notes that some issues of concern previously raised by the WP29 and the EDPB in relation to the Privacy Shield principles remain valid. In particular, these relate to the rights of data subjects (e.g. some exceptions to the right of access and the timing and modalities for the right to object), the absence of key definitions, the lack of clarity in relation to the application of the DPF Principles to processors, and the broad exemption for publicly available information⁶.

The EDPB would also like to reiterate that the level of protection of individuals whose data is transferred must not be undermined by onward transfers from the initial recipient of the transferred data⁷. The EDPB invites once more the Commission to clarify that the safeguards imposed by the initial recipient on the importer in the third country must be effective in light of third country legislation, prior to an onward transfer in the context of the DPF.

Rapid developments in the field of automated decision-making and profiling - increasingly by means of AI technologies- call for particular attention. The EDPB welcomes the Commission's references to specific safeguards provided by relevant US law in different fields⁸. However, the level of protection for individuals seems to vary according to which sector-specific rules - if any- apply to the situation at hand. The EDPB maintains that specific rules concerning automated decision-making are needed in order to provide sufficient safeguards, including the right for the individual to know the logic involved, to challenge the decision and to obtain human intervention when the decision significantly affects him or her.

The EDPB recalls the importance of effective oversight and enforcement of the DPF and considers that compliance checks as regards more substantive requirements are crucial. These aspects will be closely monitored by the EDPB, including in the context of the periodic reviews. The EDPB takes note of the renewed commitments in the letters from the Federal Trade Commission ('FTC')⁹ and the Department

³ This is the case for the terms 'agent' and 'processor'. Moreover, the concept of 'human resources (HR) data' still needs to be discussed with US authorities.

⁴ For instance, the clarification that key-coded data are personal data.

⁵ Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016 (hereinafter, 'WP29 Opinion 01/2016').

⁶ EU-U.S. Privacy Shield - Third Annual Joint Review, EDPB report adopted on 12 November 2019, para. 11.

⁷ GDPR Adequacy Referential, 3.A.9.

⁸ Draft Decision, Recital 35.

⁹ Draft Decision, Annex IV.

of Transportation ('DOT')¹⁰ as regards enforcement e.g. to prioritise the investigation of alleged DPF violations.

The EDPB notes that seven redress avenues are provided to EU data subjects, if their personal data are processed in violation of the DPF. These redress mechanisms are the same as those included in the former Privacy Shield, which had been subject to comments by the WP29¹¹. The effectiveness of these redress mechanisms will be closely monitored by the EDPB, including in the context of the periodic reviews.

1.2. Access and use of personal data transferred from the European Union by public authorities in the US

In the Draft Decision, the European Commission concludes that "any interference in the public interest, in particular for criminal law enforcement and for national security purposes, by U.S. public authorities with the fundamental rights of the individuals whose personal data are transferred from the Union to the United States under the EU-U.S. Data Privacy Framework, will be limited to what is strictly necessary to achieve the legitimate objective in question, and that effective legal protection against such interference exists"¹².

The European Commission reaches its conclusion after an extensive assessment of the Executive Order 14086 enhancing safeguards for U.S. signals intelligence activities (EO 14086). The EO 14086 was issued by the U.S. President on 7 October 2022, following negotiations of the European Commission with the U.S. Government in the wake of the invalidation of the previous adequacy decision, called the Privacy Shield, by the Court of Justice of the European Union (CJEU).

The EDPB would welcome that not only the entry into force but also the adoption of the decision are conditional upon *inter alia* the adoption of updated policies and procedures to implement EO 14086 by all US intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share this assessment with the EDPB.

With regard to governmental access to personal data transferred to the U.S., the EDPB has focussed its analysis on the assessment of the new EO 14086, as it is effectively meant to address and remedy the deficits identified by the CJEU in its Schrems II ruling when it found the previous adequacy decision to be invalid.

The EDPB recognises that the U.S. legal framework for signals intelligence activities has been amended by adoption of EO 14086 and regards the additional safeguards included in this order as a significant improvement. The EO 14086 introduces the concepts of necessity and proportionality into the U.S. legal framework on signals intelligence, and it provides, if the EU were to be designated as a qualifying regional economic integration organisation, a new redress mechanism for EU individuals. The EDPB considers the new redress mechanism to be significantly improved compared to the previous so-called Ombudsperson mechanism under the Privacy Shield. In contrast to the previous legal framework, which did not create rights for EU individuals, as was explicitly noted by the CJEU, the new EO 14086 creates such entitlements, and it provides more safeguards for the independence of the Data Protection Review Court, and more effective powers to remedy violations.

When comparing the additional safeguards included in EO 14086 to what the EDPB has framed the European Essential Guarantees (EEGs), as the standard elaborated on the basis of the jurisprudence of

¹⁰ Draft Decision, Annex V.

¹¹ See in particular WP29 Opinion 01/2016, Section 2.2.6 (a).

¹² Draft Decision, Recital 195.

the CJEU and the European Court of Human Rights (ECtHR), the EDPB has still identified in its assessment a number of points for additional clarifications, for attention or for concern. These points reflect that, while the EDPB based its opinion on the Schrems II ruling, the scope of the EDPB's assessment necessarily includes considerations that go beyond the specific findings in the Schrems II judgment.

The EDPB sees a need for further clarification on questions, in particular, relating to "temporary bulk collection", and to the further retention and dissemination of the data collected (in bulk) in the U.S. legal framework.

As the test of essential equivalence is not a test of identity, and as the safeguards included in the new legal framework on signals intelligence have been strengthened, the EDPB's main point of attention and of concern is focused on an assessment of the safeguards in their entirety, following a holistic approach covering the safeguards for the entire cycle of processing, from the collection of data to the dissemination of data, and including the elements of oversight and redress.

In this regard, the EDPB emphasises the following findings:

While the EDPB recognises that the EO 14086 introduces the concepts of necessity and proportionality in the legal framework of signals intelligence, it underlines the need to closely monitor the effects of these amendments in practice, including the review of internal policies and procedures implementing the EO's safeguards at agency level.

The EDPB also welcomes the fact that the EO 14086 contains a list of specific purposes for which collection can and cannot take place, while noting the objectives may be updated with additional – not necessarily public – objectives in the light of new national security imperatives.

As a deficit in the current framework, the EDPB has in particular identified that the U.S. legal framework, when allowing for the collection of bulk data under Executive Order 12333, lacks the requirement of prior authorisation by an independent authority, as required in the most recent jurisprudence of the ECtHR, nor does it provide for a systematic independent review *ex post* by a court or an equivalently independent body. With regard to prior independent authorisation of surveillance under Section 702 FISA, the EDPB regrets that the FISA Court ('FISC') does not review a programme application for compliance with the EO 14086 when certifying the programme authorising the targeting of non-U.S. persons, even though the intelligence authorities carrying out the programme are bound by it. In the view of the EDPB, the additional safeguards contained in this order should nevertheless be taken into account including by the FISC. The EDPB recalls that reports of the Privacy and Civil Liberties Oversight Board ('PCLOB') would be particularly useful to assess how the safeguards of the EO 14086 will be implemented and how these safeguards are applied when data is collected under Section 702 FISA and EO 12333.

On the redress mechanism, the EDPB recognises significant improvements relating to the powers of the Data Protection Review Court ('DPRC') and its enhanced independence compared to the Ombudsperson. The EDPB also recognises the additional safeguards foreseen in the new redress mechanism such as the role of the special advocates that includes advocating regarding the complainant's interest as well as the review of the redress mechanism by PCLOB. While taking into account the nature of national security and the safeguards provided in EO 14086, the EDPB is nevertheless concerned about the general application of the standard response of the DPRC notifying the complainant that either no covered violations were identified or a determination requiring appropriate remediation was issued, and its non-appealability, taken together. Given the importance

of the redress mechanism, the EDPB calls on the Commission to closely monitor the practical functioning of this mechanism.

The EDPB expects the Commission to follow up on their commitment to suspend, repeal or amend the adequacy decision on grounds of urgency, in particular if the U.S. Executive would decide to restrict the safeguards included in the EO¹³.

Overall, the EDPB positively notes the substantial improvements the EO offers compared to the previous legal framework, in particular as regards the introduction of the principles of necessity and proportionality and the individual redress mechanism for EU data subjects. Given the concerns expressed and the clarifications required, the EDPB suggests these concerns should be addressed and that the Commission provides the requested clarifications in order to solidify the grounds for the Draft Decision and to ensure a close monitoring of the concrete implementation of this new legal framework, in particular the safeguards it provides, in the future joint reviews.

¹³ Draft Decision, Recital 212.

Table of contents

1	INTRODUCTION	9
1.1	US data protection framework.....	9
1.2	Scope of the EDPB's assessment	11
1.3	General comments and concerns	13
1.3.1	Assessment of the domestic law	13
1.3.2	International commitments entered into by the U.S.	13
1.3.3	Progress in the area of US data protection legislation	14
1.3.4	Scope of the Draft Decision.....	14
1.3.5	Limitations to the duty to adhere to the DPF Principles.....	14
1.3.6	Changes with regard to the 'Privacy Shield'	15
1.3.7	Lack of clarity in the documents of the DPF	15
2	GENERAL DATA PROTECTION ASPECTS.....	16
2.1	Content principles.....	16
2.1.1	Concepts.....	16
2.1.2	The purpose limitation principle	16
2.1.3	Rights of access, rectification, erasure and objection	17
2.1.4	Restrictions on onward transfers	18
2.1.5	Automated decision-making and profiling	19
2.2	Procedural and Enforcement Mechanisms.....	20
2.3	Redress mechanisms	21
3	ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE US.....	22
3.1	Access and use for criminal law enforcement purposes	22
3.1.1	Access by law enforcement authorities to personal data should be based on clear, precise and accessible rules	22
3.1.2	Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated	23
3.1.3	An independent oversight mechanism should exist	24
3.1.4	Effective remedies need to be available to the individual	25
3.1.5	Further use of the information collected.....	26
3.2	Access and use for national security purposes.....	26
3.2.1	Guarantee A - Processing should be in accordance with the law and based on clear, precise and accessible rules	28
3.2.2	Guarantee B - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated	31

3.2.3	Guarantee C - Oversight	40
3.2.4	Guarantee D - Effective remedies need to be available to the individual.....	45
4	IMPLEMENTATION AND MONITORING OF THE DRAFT DECISION.....	53

The European Data Protection Board

The European Data Protection Board has adopted the following statement:

Having regard to Article 70(1)(s) of Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter ‘GDPR’)¹,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018²,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING OPINION

1 INTRODUCTION

1.1 US data protection framework

1. The United States (‘US’) and the European Union (‘EU’) have different approaches to privacy and data protection. While privacy and data protection in the EU are fundamental rights guaranteed in Articles 7 and 8 of the European Charter of Fundamental Rights, data protection in the US is generally approached from a consumer protection perspective. As a result, regulatory approaches in the US and EU differ³.
2. Differing from the EU comprehensive approach taken by the GDPR, in the US, no comprehensive general law on data protection exists at federal level. The protection of privacy in the US is rather realised by a sectoral and state approach. For instance, some specific sectors are covered by specific acts, e.g.:
 - Health Insurance Portability and Accountability Act (HIPAA)⁴

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1.

² References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

³ See also European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, published on 13 December 2022 (hereinafter, the ‘Draft Decision’), Annex I, Section I.

⁴ The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a U.S. federal law. It creates national standards to protect patients' sensitive health information. The goal of HIPAA is to adequately protect individuals' health information, while allowing health information to flow for the delivery and promotion of high quality health care. HIPAA governs the use and disclosure of health information by entities subject to the Privacy Rule. It also includes standards for the rights of individuals to understand and control how their health information is used.

- Children's Online Privacy Protection Act (COPPA)⁵
 - Gramm-Leach-Billey Act (GLBA)⁶
3. In the field of government access to personal data transferred from the EU to the US a number of different legal bases, limitations and safeguards apply. The legal processes for access to information for law enforcement purposes stem either from the U.S. Constitution directly (the Fourth Amendment), from statutory and procedural law or from Guidelines and Policies of the Department of Justice at federal level or at state level. Access to information for national security purpose is governed by several legal instruments and in particular by the Foreign Intelligence Surveillance Act (FISA), the Executive Order 12333, the recently adopted Executive order 14086 as well as the Attorney General regulation ('AG Regulation')⁷ establishing a Data Protection Review Court ('DPRC').
4. On 13 December 2022, the Commission issued its draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework ('the Draft Decision'), which contains in its annex the EU-US Data Privacy Framework ('the DPF'). For the reasons explained above, the Draft Decision is not based on a specific and comprehensive federal legal framework, but on the DPF.
5. The DPF works as follows: '*The U.S. Department of Commerce ("the Department") is issuing the EU-U.S. Data Privacy Framework Principles, including the Supplemental Principles (collectively "the Principles") and Annex I of the Principles ("Annex I"), under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512)*'⁸.
6. The development of the 'Principles' ('the DPF Principles') was conducted under consultation of the European Commission ('the Commission'), industry and other stakeholders in order to achieve the goal of the facilitation of EU–U.S. trade and commerce⁹, while ensuring that data subjects are provided with a level of protection that is essentially equivalent to that guaranteed in the EU.
7. The DPF Principles are described as a 'key component' of the DPF. On the one hand, they provide a 'ready-to-use mechanism' for data transfers from the EU to the US. On the other hand, personal data transferred from the EU to the US is safeguarded and protected as required by EU law.

<https://www.hhs.gov/hipaa/for-professionals/privacy/index.html>; <https://www.justice.gov/opcl/privacy-act-1974>.

⁵ The primary goal of COPPA is to place parents in control over what personal information is collected from their children under 13 from operators of child-directed websites and online services (including mobile apps and IoT devices, such as smart toys) or general audience sites. COPPA requires that these operators provide parental notice and obtain verifiable parental consent. This also applies to data from foreign children if the websites or services are operated in the U.S. and subject to COPPA. At the same time, the regulations also apply to foreign-based websites and services if they are directed at children in the U.S. See: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions> and Draft Decision, Annex IV, p. 3.

⁶ One of the goals of the Gramm-Leach-Bliley Act is to protect consumer privacy in the financial sector. The GLB Act requires financial institutions to explain to their customers their information-sharing practices and to create safeguards to protect customer information (e.g., for companies regulated by the FTC under the FTC Safeguards Rule). <https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act>

⁷ Attorney General Order No. 5517-2022, which amends US Department of Justice regulations as authorised and directed by EO 14086.

⁸ Draft Decision, Annex I, Section I.

⁹ *Ibid.*

8. The DPF is only applicable for US organisations who have self-certified themselves according to the requirements of the framework ('DPF Organisations'). For the time being, this is only possible if they fall under the jurisdiction of the Federal Trade Commission ('FTC') or the Department of Transportation ('DoT'). In the future, other statutory bodies – with competence to supervise the implementation of the DPF Principles - might be added in a future annex.
9. It is explained by the DPF Principles that the conditions of the framework are enforceable by (i) the FTC under Section 5 of the Federal Trade Commission Act (FTC Act) prohibiting unfair or deceptive acts in or affecting commerce¹⁰, (ii) the DoT under 49 U.S.C. § 41712 prohibiting a carrier or ticket agent from engaging in an unfair or deceptive practice in air transportation for the sale or of air transportation or (iii) under other laws or regulations by which such acts are prohibited.
10. It is pointed out in the DPF Principles that neither the GDPR is affected in its application nor existing privacy obligations, otherwise applied under US law, are limited by the DPF Principles.

1.2 Scope of the EDPB's assessment

11. The Draft Decision reflects the Commission's assessment of the DPF, which is the outcome of discussions with the US government. In accordance with Article 70(1)(s) GDPR, the EDPB is expected to provide an opinion on the Commission's findings as regards the adequacy of the level of protection in a third country and, if needed, endeavour to make proposals to address any issue.
12. The EDPB welcomes the updates made to the DPF Principles¹¹, which will constitute the binding legal framework for DPF Organisations. However, the EDPB notes that the DPF Principles remain essentially the same as those under the Privacy Shield¹² (on which were based the Working Party 29 ('WP29') and EDPB annual joint reviews). The DPF Principles are also, to a large extent, the same as those of the draft Privacy Shield on which the WP29 based its 2016 opinion¹³ ('the WP29 Opinion 01/2016'). For those DPF Principles that are substantially unchanged, the EDPB considers not necessary to repeat all comments previously made by the WP29. The EDPB has decided to focus on specific aspects that it considers to be even more relevant today, in view of the evolution of the legal and technological environment.
13. In addition, in line with the jurisprudence of the CJEU¹⁴, a very important part of the analysis covers the legal regime of government access to personal data transferred to the US.
14. In its assessment, the EDPB took into account the applicable European data protection framework, including Articles 7, 8 and 47 of the EU Charter of Fundamental Rights ('the Charter'), respectively protecting the right to private and family life, the right to protection of personal data and the right to an effective remedy and fair trial, and Article 8 of the European Convention on Human Rights ('ECHR') protecting the right to private and family life. In addition to the above, the EDPB considered the

¹⁰ 15 U.S.C. § 45 (a).

¹¹ For instance, the clarification that key-coded data are personal data.

¹² Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, OJ L 207, 1.8.2016, p. 1.

¹³ Article 29 Working Party, Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016 (hereinafter, 'WP29 Opinion 01/2016').

¹⁴ In particular: Judgment of the Court of Justice of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner*, C-392/14, ECLI:EU:C:2015:650, and Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559.

requirements of the GDPR, the relevant case law and the Adequacy Referential adopted by the EDPB ('the GDPR Adequacy Referential')¹⁵.

15. The objective of this exercise is to provide the Commission with an opinion on the assessment of the adequacy of the level of protection provided by the DPF. The concept of 'adequate level of protection', which already existed under Directive 95/46, has been further developed by the CJEU. It is therefore important to recall the standard set by the CJEU in its Schrems I¹⁶ (invalidating the 'Safe Harbor') and Schrems II¹⁷ (invalidating the Privacy Shield) judgments.
16. In its Schrems I judgment, the CJEU ruled that, while the 'level of protection' in the third country must be 'essentially equivalent' to that guaranteed in the EU – *'the means to which that third country has recourse, in this connection, for the purpose of such a level of protection may differ from those employed within the EU'*¹⁸. Therefore, the objective is not to mirror point by point the European legislation, but to establish the essential and core requirements of the legislation under examination. Adequacy can be achieved through a combination of rights for the data subjects and obligations on those who process personal data, or who exercise control over such processing and supervision by independent bodies. However, data protection rules are only effective if they are enforceable and followed in practice. It is therefore necessary to consider not only the content of the rules applicable to personal data transferred to a third country or an international organisation, but also the system in place to ensure the effectiveness of such rules. Efficient enforcement mechanisms are of paramount importance to the effectiveness of data protection rules¹⁹.
17. In its Schrems II decision, the CJEU found that the laws on the basis of which U.S. intelligence authorities can access personal data transferred to the U.S. (Section 702 FISA/E.O. 12333) disproportionately restrict the rights enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights (the Charter) and are thus not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter²⁰.
18. Moreover, the CJEU stated that the previous legal framework did not provide guarantees essentially equivalent to those required by Article 47 of the Charter as the Ombudsperson mechanism could not compensate, for the fact that neither PPD-28 nor E.O. 12333 grant non-U.S. persons an effective remedy²¹. The Ombudsperson lacked independence from the executive and the power to adopt binding decisions on U.S. intelligence services²².
19. EO 14086, which generally replaces PPD-28, introduced two new requirements under US law which echo the CJEU Schrems II judgment: on the one hand, that signals intelligence activities shall be conducted only as far as necessary to advance a validated intelligence priority collection and only to

¹⁵ Art. 29 Working Party, Adequacy Referential, WP 254 rev.01, 28 November 2017, as last revised and adopted on 6 February 2018, endorsed by the EDPB on 25 May 2018 (hereinafter 'GDPR Adequacy Referential').

¹⁶ CJEU Schrems I Judgment of the Court of Justice of 6 October 2015, *Maximilian Schrems v Data Protection Commissioner*, C-392/14, ECLI:EU:C:2015:650 (hereinafter, 'CJEU Schrems I Judgment').

¹⁷ Judgment of the Court of Justice of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18, ECLI:EU:C:2020:559 (hereinafter, 'CJEU Schrems II Judgment').

¹⁸ CJEU Schrems I Judgment, paras. 73-74.

¹⁹ GDPR Adequacy Referential, p.2.

²⁰ CJEU Schrems II Judgment, paras. 184-185.

²¹ CJEU Schrems II Judgment, para. 192.

²² CJEU Schrems II Judgment, para. 195.

the extent and in a manner that is proportionate to the validated intelligence priority; and on the other hand, a redress mechanism.

20. In this opinion, the EDPB particularly assesses to which extent the DPF as well as the recently adopted EO 14086 effectively address the findings made by the CJEU in its judgment.

1.3 General comments and concerns

1.3.1 Assessment of the domestic law

21. The EDPB understands that the assessment contained in the Draft Decision relates to the DPF Principles. Nevertheless the EDPB would welcome some information about the US legal context, in which the DPF Organisations are operating. This would allow a better understanding of the interaction of the DPF with US law. For example, in Annex I 1²³ it is determined that the DPF Principles do not '[...] limit privacy obligations that otherwise apply under U.S. law', without describing these obligations.

1.3.2 International commitments entered into by the U.S.

22. According to Article 45(2)(c) GDPR and the GDPR Adequacy Referential, when assessing the adequacy of the level of protection of a third country, the Commission shall take into account, among others, the international commitments the third country has entered into, or other obligations arising from the third country's participation in multilateral or regional systems, in particular in relation to the protection of personal data, as well as the implementation of such obligations.
23. The US is a party to several international agreements that guarantee the right to privacy, such as the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of Persons with Disabilities (Article 22) and the Convention on the Rights of the Child (Article 16). Furthermore, the US, as an OECD member, adheres to the OECD Privacy Framework, in particular the Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data. On 14 December 2022, the OECD 'Declaration on Government Access to Personal Data held by Private Sector Entities' was adopted by Ministers and high-level representatives of OECD Members and the European Union. The US is also a party to the Budapest Convention on Cybercrime.
24. In addition, the US is a member of the Asia-Pacific Economic Cooperation ('APEC') Cross-Border Privacy Rules (CBPR) system, which is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally recognized privacy rules. These privacy rules have been endorsed by APEC Leaders.
25. The EDPB also takes note of the participation of the US as Observer State in the work of the Consultative Committee of the Council of Europe Convention 108.
26. Furthermore, the EDPB takes note of and welcomes the continuous engagement of US bodies in the 2021 newly established format of the 'Roundtable of G7 Data Protection and Privacy Authorities' (G7 DPA Roundtable), which convenes independent data protection and privacy supervisory authorities of G7 countries. In this context, they have supported, for example, the latest G7 DPA Roundtable

²³ Draft Decision, Annex I, Section I, last sentence.

communiqué²⁴ adopted on 8 September 2022 in Bonn, Germany, which focussed on the concept of ‘Data Free Flow with Trust’.

1.3.3 Progress in the area of US data protection legislation

27. The EDPB takes particular note of developments in data privacy legislation at state level in the US. The EDPB welcomes the adoption of data protection laws that have entered into force or will enter into force by 2023 in five States (California, Colorado, Connecticut, Virginia and Utah)²⁵.
28. The EDPB also notes that corresponding initiatives for further State laws have already been launched in many other US States.
29. Furthermore, the EDPB explicitly welcomes the efforts regarding the bipartisan initiative for a federal data protection law, the American Data Privacy and Protection Act (ADPPA).

1.3.4 Scope of the Draft Decision

30. According to Article 1 of the Draft Decision, the Commission concludes that the US ensures an adequate level of protection for personal data transferred from the EU to organisations in the United States that are included in the ‘Data Privacy Framework List’, maintained and made publicly available by the U.S. Department of Commerce (‘DoC’), in accordance with Section I.3 of Annex I²⁶.
31. The DPF is available to companies under the jurisdiction of the FTC or the DoT. It is pointed out that other US statutory bodies with similar powers might be added in future²⁷.

1.3.5 Limitations to the duty to adhere to the DPF Principles

32. Annex I, I.5. provides that adherence to the DPF Principles by DPF Organisations may be limited, among others, (i) to the extent necessary to comply with a court order or to meet public interest, law enforcement²⁸, or national security requirements²⁹ (including where statute or government regulation create conflicting obligations) and (ii) by statute, court order, or government regulation that creates explicit authorisations, provided that, in exercising any such authorisation, a DPF organisation can demonstrate that its non-compliance with the DPF Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation.

²⁴ Roundtable of G7 Data Protection and Privacy Authorities, Promoting Data Free Flow with Trust and knowledge sharing about the prospects for International Data Spaces, 8 September 2022, https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1.

²⁵ California Consumer Privacy Act (2018; effective Jan. 1, 2020); California Privacy Rights Act (2020; fully operative Jan. 1, 2023); Colorado Privacy Act (2021; effective July 1, 2023); Connecticut Data Privacy Act (2022; effective July 1, 2023); Virginia Consumer Data Protection Act (2021; effective Jan. 1, 2023); Utah Consumer Privacy Act (2022; effective Dec. 31, 2023).

²⁶ Draft Decision, Final Considerations, Article 1, p. 57. The EDPB understands that the Draft Decision will not cover transfers from entities located outside the EU but subject to the GDPR by virtue of Article 3(2) GDPR to certified entities in the US.

²⁷ Draft Decision, Annex I, Section I.2.

²⁸ See Section 3.1 of the present opinion for more comments on the use of personal data covered by the EU-U.S. DPF for law enforcement purposes.

²⁹ See Section 3.2 of the present opinion for more comments on the use of personal data covered by the EU-U.S. DPF for national security purposes.

33. Without full knowledge of US law at both the federal and state level, it is difficult for the EDPB to assess in detail the scope of the exemptions listed in this paragraph. Therefore, the EDPB recommends that the Commission includes in the Draft Decision clarification on the scope of the exemptions, including on the applicable safeguards under US law, in order to better identify the impact of these exemptions on the level of protection for data subjects. The EDPB also underlines that the Commission should be informed of and monitor the application and adoption of any statute or government regulation that would affect adherence to the DPF Principles.

1.3.6 Changes with regard to the 'Privacy Shield'

34. The EDPB welcomes the effort made to address the requirements of the Schrems II judgment. Nevertheless, the EDPB would have welcomed, if more issues identified (i) in the WP29 Opinion 01/2016 and (ii) in the past joint reviews³⁰, would have been also addressed on the occasion of the negotiations of the DPF.
35. The EDPB also notes that despite a number of changes and additional explanations made in the recitals of the Draft Decision, the DPF Principles to which the DPF Organisations have to adhere remain essentially unchanged with regard to those applicable under the Privacy Shield.

1.3.7 Lack of clarity in the documents of the DPF

36. The EDPB notes that the structure of the annexes and their numbering makes the information rather difficult to find and refer to. This contributes to an overall complex presentation of the new framework, which compiles in its annexes documents of different legal value, and may not favour a good understanding of the DPF Principles by data subjects, DPF Organisations, and EU Data Protection Authorities ('EU DPA's').
37. The EDPB also stresses that the terminology should be used consistently throughout the DPF. This is currently not the case, for example, for the notion of 'processing'. Indeed, some of the parts of the DPF enumerate some types of data processing operations instead of making use of the term 'processing'. This may result in legal uncertainty and possible loopholes in the protection³¹.
38. The EDPB welcomes that definitions of some of the terms used are included in the DPF³². However, this is not the case for some other essential terms such as at least 'agent' or 'processor', which in the view of the EDPB warrant a clear and specific definition in Annex I, I 8 of the DPF, and on which both the US and the EU agree, in order to avoid confusion at a later stage for DPF Organisations relying on the DPF, the supervisory authorities and the general public.

³⁰ Annual reviews: EU-U.S. Privacy Shield – First Annual Joint Review, WP 255, WP29 Report Adopted on 28 November 2017 (hereinafter 'First Joint Review report'); EU-U.S. Privacy Shield - Second Annual Joint Review, EDPB Report Adopted on 22 January 2019 (hereinafter 'Second Joint Review report'); EU-U.S. Privacy Shield - Third Annual Joint Review, EDPB Report Adopted on 12 November 2019 (hereinafter 'Third Joint Review report').

³¹ For instance (i) according to the wording of the Draft Decision, Annex I, Section III.6.(f), the DPF Principles would be applicable only where the organisation "stores, uses or discloses" the received data (i.e. not for other operations covered by the term 'processing', such as collecting, recording, alteration, retrieval, consulting, erasure.) and (ii) according to the Draft Decision, Annex I , Section II.4.(a), data security would be imposed only for 'creating, maintaining, using or disseminating' personal information.

³² Draft Decision, Annex I, I 8.

39. As to the question of diverging interpretations in the EU and the US on the concept of human resources (HR) data, the EDPB agrees with the Commission’s third review report on the objective of continuing the discussions with US authorities³³.

2 GENERAL DATA PROTECTION ASPECTS

2.1 Content principles

2.1.1 Concepts

40. Based on the GDPR Adequacy Referential, basic data protection concepts and/or principles should exist in the third country’s legal framework. Although these do not have to mirror the GDPR terminology, they should reflect and be consistent with the concepts enshrined in European data protection law. For example, the GDPR includes the following important concepts: ‘personal data’, ‘processing of personal data’, ‘data controller’, ‘data processor’, ‘recipient’ and ‘sensitive data’. The EDPB welcomes that definitions of the terms ‘personal data’, ‘processing’ and ‘controller’ are included in the DPF, as it was the case in the Privacy Shield.
41. The EDPB notes that the extent to which the DPF Principles are applicable to DPF Organisations receiving personal data from the EU for ‘mere processing’ purposes (referred to as ‘agents’ or ‘processors’) remains unclear. The DPF does not distinguish between DPF Principles applicable to agents and DPF Principles applicable to controllers, while several of the obligations included in the DPF Principles are not suitable for agents/processors. For instance, an agent/processor should not be able to provide individuals with all the elements of the full Notice as required by the Notice principle (e.g. the purposes for which it collects and uses personal information about them)³⁴, as an agent/processor cannot determine alone the means and purposes of the processing³⁵.

2.1.2 The purpose limitation principle

42. The GDPR Adequacy Referential, in line with the GDPR, provides that personal data should be processed for a specific purpose and subsequently used only insofar as this is not incompatible with the purpose of the processing.
43. The Data Integrity and Purpose Limitation principle states that an organisation may not process personal information in a way incompatible with the purposes for which it has been collected or subsequently authorised by the individual³⁶. The EDPB notes that different terminology is used under the Notice, the Choice and the Data Integrity and Purpose Limitation principles. As noted by the WP29 and despite useful clarification in the recitals of the Draft Decision, terms such as ‘different purposes’, ‘materially different’ purposes, or ‘a use that is not consistent with’ are used in the DPF without a clear definition of these concepts therein and might lead to legal uncertainty.

³³ Third Joint Review Report, pages. 5, 15-16 and 30; See also Commission Staff Working Document Accompanying the document Report From The Commission to the European Parliament and The Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, p.17-18.

³⁴ Draft Decision, Annex I, Section II.1.(a).

³⁵ Please also refer to the WP29 Opinion 01/2016, p.16.

³⁶ Draft Decision, Annex I, Section II.5.

2.1.3 Rights of access, rectification, erasure and objection

44. In the DPF, data subjects' rights to access, rectification and erasure are addressed by the Access principle³⁷.
45. The Access principle remains unchanged compared to the Privacy Shield. Consequently, some points of concern expressed in the WP29 Opinion 01/2016 are still valid as detailed below.
46. With regard to individuals' right of access, the EDPB finds it necessary to reiterate that the details of the obligation to answer requests from individuals would be better inserted in the main text of the principle (they are still described in a footnote only³⁸). Also, it should be clear that access should be provided to the extent that a DPF Organisation processes personal information, not only when it 'stores' it³⁹. In the view of the EDPB, the current wording could lead to a narrow interpretation of the right of access.
47. In relation to the list of exceptions to the right of access⁴⁰, some still tend to incline the balance towards the interests of DPF organisations. It remains a concern to the EDPB that, in those cases, there seems to be no requirement to take into account the rights and interests of the individual⁴¹.
48. Another exception, which has been subject to previous concern by the WP29⁴² and which to the EDPB seems overly broad, is the exception to the right of access for publicly available information and information from public records⁴³. The EDPB has repeatedly stated that, according to EU law, data subjects always have the right of access their data regardless of whether or not the personal data have been published. If requests for access were to be rejected on the grounds that the data were obtained from publicly available sources or public records, the individuals would lose the ability to control the accuracy of the data and to control whether the data were lawfully made public in the first place.
49. The EDPB recalls that the right of access is enshrined in Article 8(2) of the Charter. While this is not an absolute right, it is fundamental for the right to the protection of personal data as it facilitates the exercise of the other rights of the data subject, such as correction and erasure, and the right to object⁴⁴.
50. In addition to the rights of access, erasure and deletion, data subjects should have the right to object on compelling legitimate grounds relating to their particular situation, at any time, to the processing of their data under specific conditions established in the third country legal framework⁴⁵.
51. With the Choice principle, the DPF provides for a right to object (opt-out) to disclosure of personal information to a third party or to the use of personal information for a purpose materially different⁴⁶. In addition, individuals benefit from a right to opt-out to the use of their personal information for direct marketing purpose at any time⁴⁷. Except for the context of direct marketing purposes, the modalities,

³⁷ Draft Decision, Annex I, II.6 and III.8.a.(i).

³⁸ Draft Decision, Annex I, III.8.a.(i)1. - footnote 14.

³⁹ Draft Decision, Annex I, III.8.d(ii).

⁴⁰ Draft Decision, Annex I, III.8.e.

⁴¹ WP29 Opinion 01/2016, pt. 2.2.5.

⁴² WP29 Opinion 01/2016, pt. 2.2.9.

⁴³ Draft Decision, Annex I, III.15.d-e.

⁴⁴ WP29 Opinion 01/2016, pt. 2.2.5.

⁴⁵ GDPR Adequacy Referential, section 3.A.8.

⁴⁶ Draft Decision, Annex I, II.2.(a).

⁴⁷ Draft Decision, Annex I, III.12.(a).

in particular of the timing, for exercising the right to object, are not detailed. Therefore, the EDPB invites the Commission to clarify how individuals can exercise their right to object.

52. As stated in the WP29 Opinion 01/2016, the EDPB considers that the simple reference to the existence of this right in the privacy policy cannot be sufficient. An individualised opportunity to exercise this right should be offered not only in case of disclosure or re-use of personal information. The EDPB emphasises that a general right to object on compelling legitimate grounds relating to the data subject's particular situation should be offered within the DPF. The EDPB recommends that such right to object be guaranteed at any given moment, and that this right is not limited to the use of the data for direct marketing⁴⁸.
53. In relation to HR data, the EDPB appreciates the clarifications of the Commission as regards the application of the Notice and Choice Principles in the situation where a certified U.S. organisation intends to use HR data for a different, non-employment-related purpose, such as marketing communications⁴⁹. However, the EDPB maintains that further processing of HR data for non-employment-related purposes will in most cases be considered incompatible with the original purpose, and that consent will rarely be entirely free when given in an employment context.
54. The EDPB also reiterates the concerns of the WP29 in relation to the exemption to the Notice and Choice Principles for HR data '*to the extent and for the period necessary to avoid prejudicing the ability of the organisation in making promotions, appointments or other similar employment decisions*',⁵⁰ which to the EDPB appears broad and vague⁵¹.

2.1.4 Restrictions on onward transfers

55. Onward transfers of the personal data by the initial recipient of the original data transfer should be permitted only where the further recipient (i.e. the recipient of the onward transfer) is also subject to rules (including contractual rules) affording an adequate level of protection and following the relevant instructions when processing data on the behalf of the data controller. The level of protection of individuals whose data is transferred must not be undermined by the onward transfer. The initial recipient of the data transferred from the EU shall be liable to ensure that appropriate safeguards are provided for onward transfers of data in the absence of an adequacy decision. Such onward transfers of data should only take place for limited and specified purposes and as long as there is a legal ground for that processing⁵².
56. According to the Accountability for Onward Transfers principle of the DPF, onward transfers can only take place for limited and specified purposes, on the basis of a contract between the DPF Organisation and the third party (or comparable arrangement within a corporate group) and only if that contract requires the third party to provide the same level of protection as the one guaranteed by the DPF Principles⁵³.

⁴⁸ WP29 Opinion 01/2016, pt. 2.2.2.

⁴⁹ Draft Decision, Annex I, III.9.b.(i) and Recital 15 and footnote 27.

⁵⁰ Draft Decision, Annex I, III.9.b.iv.

⁵¹ WP29 Opinion 01/2016, pt. 2.2.7.

⁵² GDPR Adequacy Referential, section 3.A.9.

⁵³ Draft Decision, Annex I, II.3.

57. The EDPB would like to reiterate the concerns expressed in the WP29 Opinion 01/2016 regarding the exemption to the need of contract for intra-group transfers between controllers⁵⁴. In relation to HR data, the EDPB still does not understand the rationale for the exemption from the obligation to enter into a contract with a third-party controller in case of onward transfers for 'occasional employment-related operational needs'⁵⁵.
58. Furthermore, the EDPB would like to repeat the WP29 request⁵⁶ that organisations bound by the framework should assess prior to an onward transfer that the mandatory requirements of the third country's national legislation applicable to the recipient would not undermine the continuity of protection of the data subjects whose data are transferred⁵⁷.
59. The EDPB maintains that onward transfers of personal data to third countries could lead to interferences with individuals' fundamental rights and invites the Commission to clarify that the safeguards imposed by the initial recipient on the importer in the third country must be effective in light of third country legislation, prior to an onward transfer in the context of the DPF⁵⁸.

2.1.5 Automated decision-making and profiling

60. Decisions based solely on automated processing (automated individual decision-making), including profiling, which produce legal effects or significantly affect the data subject, can take place only under certain conditions established in the third country legal framework. In the European framework, such conditions include, for example, the need to obtain the explicit consent of the data subject or the necessity of such a decision for the conclusion of a contract. If the decision does not comply with such conditions as laid down in the third country legal framework, the data subject should have the right not to be subject to it. The law of the third country should, in any case, provide for necessary safeguards, including the right to be informed about the specific reasons underlying the decision and the logic involved, to correct inaccurate or incomplete information, and to contest the decision where it has been adopted on an incorrect factual basis⁵⁹.
61. The DPF does not provide for any specific legal guarantees where individuals are subject to decisions which produce legal effects concerning or significantly affecting them and which are based solely on automated processing of data intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability or conduct.

⁵⁴ Draft Decision, Annex I, III.10.b(i), which refers to 'or other intra-group instruments (e.g. compliance and control programs) which apparently do not need to be binding.'

⁵⁵ Draft Decision, Annex I, III.9.e(i), referring to examples such as insurance coverage.

⁵⁶ WP29 Opinion 01/2016, pt. 2.2.3, p. 21.

⁵⁷ In light of the *Schrems II* judgment, the EDPB has further clarified the obligations for data exporters and importers in relation to onward transfers in a number of guidelines and recommendations: see EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0, adopted on 18 June 2021); Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (Adopted on 10 November 2020); Guidelines 04/2021 on Codes of Conduct as tools for transfers (Version 2.0 Adopted on 22 February 2022); Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Adopted on 14 November 2022); Guidelines 07/2022 on certification as a tool for transfers (adopted after public consultation on 14 February 2023).

⁵⁸ WP29 Opinion 01/2016, pt. 2.2.3, p. 21.

⁵⁹ GDPR Adequacy Referential, Section 3.B.3.

62. As already considered in the WP29 Opinion 01/2016 and by the EDPB in its previous opinions on the adequacy decisions relating to Japan and South Korea⁶⁰, the EDPB finds that rapid developments in the field of automated decision-making and profiling – increasingly by means of AI technologies - call for particular attention in this regard.⁶¹
63. The EDPB takes note of the Commission’s arguments, according to which the absence of specific rules on automated decision-making in the DPF is unlikely to affect the level of protection as regards personal data that has been collected in the Union (since any decision based on automated processing would typically be taken by the controller in the Union which has a direct relationship with the concerned data subject)⁶². However, in the view of the EDPB, it cannot be ruled out that automated decision-making could be used by a US-based controller on data transferred under the Draft Decision (e.g. in the context of employment, for assessing performance at work, insurance, housing).
64. The EDPB welcomes the Commission’s references to specific safeguards provided by relevant US law in different fields⁶³. However, to the EDPB, the level of protection for individuals appears to vary according to which sector-specific rules – if any – apply to the situation at hand. There is a risk that some situations will not be covered because they do not fall within the scope of the acts referred to. Furthermore, the content of individual rights in relation to automated decision-making is described differently in the various acts.
65. On this background, the EDPB considers that specific rules in the DPF concerning automated decision-making are needed in order to provide sufficient safeguards, including the right for the individual to know the logic involved, to challenge the decision and to obtain human intervention when the decision significantly affects him or her⁶⁴.

2.2 Procedural and Enforcement Mechanisms

66. The EDPB notes that the DPF continues to rely on a system of self-certification, even if the Commission refers to it as a system of ‘certification’.
67. The EDPB recalls the improvements achieved in the course of the past joint reviews. For instance, as regards the role of the DoC, on the (re-)self-certification process (...), the monitoring of companies’ compliance with the DPF Principles (e.g. through spot checks, the use of compliance questionnaires) and identifying and addressing false claims of participation (e.g. through internet searches).
68. At the same time, the WP29 and the EDPB had expressed concerns about a certain lack of oversight of compliance with the requirements of the Privacy Shield⁶⁵. In particular, the EDPB agrees with the Commission’s findings after the third annual review of the Privacy Shield that, under the Privacy Shield, spot-checks by the DoC tended to be limited to formal requirements (e.g. lack of response from

⁶⁰ EDPB Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan, adopted on 5 December 2018; EDPB Opinion 32/2021 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in the Republic of Korea, adopted on 24 September 2021.

⁶¹ See, *inter alia*, C-634/21, *OQ v Land Hesse (SCHUFA Holding and Others)*, Request for preliminary ruling (pending).

⁶² Draft Decision, Recitals 33 and 34.

⁶³ Draft Decision, Recital 35.

⁶⁴ See also Third Joint Review report, pt. 76.

⁶⁵ Third Joint Review report, pt. 7.

designated points of contact or inaccessibility of a company's privacy policy online)⁶⁶. The EDPB considers that compliance checks as regards more substantive requirements are crucial.

69. The EDPB also recalls the importance of effective oversight (including of compliance with substantive requirements) and enforcement of the DPF. This aspect will be closely monitored by the EDPB, including in the context of the periodic reviews.
70. As regards enforcement, the EDPB takes note of the renewed commitments in the letters from the FTC⁶⁷ and the DoT⁶⁸ to prioritise the investigation of alleged DPF violations, take appropriate enforcement action against entities making false or deceptive claims of participation, monitor enforcement orders concerning DPF violations and cooperate with EU DPAs. In this respect, the EDPB also recognises that the FTC has indicated that it expects to further focus its enforcement efforts on substantive violations of the DPF and that it intends to investigate (also) on its own initiative. These aspects will be closely monitored by the EDPB including in the context of the periodic reviews.

2.3 Redress mechanisms

71. The EDPB welcomes the clear presentation in the Draft Decision of the seven redress avenues provided to EU data subjects, if their personal data are processed in violation of the DPF⁶⁹.
72. These different recourse mechanisms are established in accordance with the requirements of the Recourse, Enforcement and Liability principle and the Supplemental Principle 11 on 'Dispute Resolution and Enforcement' issued by the DoC, and mentioned in Annex I to Draft Decision⁷⁰.
73. As underlined by the Commission in its Draft Decision, '*the data subject should be provided with effective administrative and judicial redress*'⁷¹. This echoes the requirement of Article 45(2)(a) GDPR, according to which the Commission, in its assessment of the adequacy of the level of protection in a third country, has to take account, in particular, of 'effective administrative and judicial redress for the data subjects whose personal data are being transferred'⁷². This requirement is also recalled by the GDPR Adequacy Referential⁷³.
74. The EDPB notes that these redress mechanisms are the same as those included in the former Privacy Shield, which had been subject to comments by the WP29⁷⁴.
75. With regard to the arbitration mechanism, the EDPB notes that this option is not available with respect to the exceptions to the DPF Principles⁷⁵ and therefore refers to its comment made in paragraph 33.

⁶⁶ Report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield (23.10.2019 COM(2019)495 final), p.4.

⁶⁷ Draft Decision, Annex IV

⁶⁸ Draft Decision, Annex V

⁶⁹ Draft Decision, Recital 67.

⁷⁰ Draft Decision, Annex I, Section II.7 and III. 11 and Annex I to Annex I.

⁷¹ Draft Decision, Recital 64.

⁷² See also Recital 141 GDPR referring to Article 47 Charter of Fundamental Rights for the right to an effective judicial remedy in the EU.

⁷³ GDPR Adequacy Referential, p.8.

⁷⁴ See in particular, WP29 Opinion 01/2016, Section 2.2.6 (a).

⁷⁵ Draft Decision, Annex I to Annex I, A.

- 76. With regard to additional avenues for judicial redress available under US law, the EDPB would also welcome further details on the legislation mentioned⁷⁶ and refer to its comment made in paragraph 21.
- 77. In addition, the EDPB welcomes the letter from the FTC describing its intent to work closely with EU DPAs⁷⁷. The EDPB also welcomes the prioritisation of complaints by the FTC although it may not give certainty to the data subject that its complaints will be dealt with in all cases.
- 78. As regards the possibility, in certain cases, for individuals to bring their complaints to an EU DPA, the EDPB would welcome further information (i) as to whether the EU DPA's possibility to give advice on remedial or compensatory measures could include recommendation for fines or the use of investigative powers and (ii) to which extent the EU DPA's action would be taken into account as evidence for enforcement action by the FTC or the DoT⁷⁸.
- 79. The effectiveness of the redress mechanisms will be closely monitored by the EDPB including in the context of the periodic reviews.

3 ACCESS AND USE OF PERSONAL DATA TRANSFERRED FROM THE EUROPEAN UNION BY PUBLIC AUTHORITIES IN THE US

3.1 Access and use for criminal law enforcement purposes

3.1.1 Access by law enforcement authorities to personal data should be based on clear, precise and accessible rules

- 80. The EDPB welcomes the more detailed information and explanations, compared to the previous adequacy decision, provided for in the Draft Decision with regard to the access and use of personal data by U.S. public authorities for criminal law enforcement purposes. The Draft Decision, in its Annex VI, contains also a letter from the U.S. Department of Justice, Criminal Division "providing a brief overview of the primary investigative tools used to obtain commercial data and other record information from corporations in the United States for criminal law enforcement or public interest (civil and regulatory) purposes, including the access limitations set forth in those authorities". According to the letter, all the legal processes described in the letter are used to obtain information from corporations in the U.S., without regard to the nationality or place of residence of the data subject and stem either from the U.S. Constitution directly (the Fourth Amendment), from statutory and procedural law or from Guidelines and Policies of the Department of Justice. This overview does not cover the national security investigative tools used by law enforcement in terrorism and other national security investigations⁷⁹.
- 81. The EDPB notes that the Draft Decision and its Annex VI discuss primarily federal law enforcement and regulatory authorities⁸⁰ and do not refer specifically to the statutes under state law that provide for these procedures to obtain information., Annex VI also mentions that "there are other legal bases for companies to challenge data requests from administrative agencies based on their specific industries

⁷⁶ Draft Decision, Recital 85.

⁷⁷ Draft Decision, Annex IV.

⁷⁸ Draft Decision, Annex I, III.5.b.(iii).

⁷⁹ Draft Decision, Footnote 1 to Annex VI.

⁸⁰ See Draft Decision, recitals 90-93.

and the types of data they possess”, giving in addition several, non-exhaustive examples, such as the Bank Secrecy Act and its implementing regulations⁸¹, the Fair Credit Reporting Act⁸², the Right to Financial Privacy Act⁸³. The EDPB notes that the applicable legal basis to a given request for access depends on the nature of the data sought, the nature of the company, the nature of the legal procedures (criminal, administrative, related to other public interest) and the nature of the entity requesting access. Since all applicable rules to limit access by law enforcement authorities to data transferred to the U.S. are based on the Constitution, on statutory law and on transparent policies of the Department of Justice, the EDPB acknowledges the accessibility of these rules and invites the Commission to reflect this element in the Draft Decision. It stems from Annex VI, these statutes apply regardless of nationality or place of residence of the data subject and generally incorporate the Fourth Amendment requirements (although they often also go beyond that and include additional protections).

82. In conclusion, the EDPB notes the more detailed assessment contained in the Draft Decision compared to the previous adequacy decision as far as access by federal law enforcement authorities is concerned. As for access by state law enforcement authorities, the EDPB also takes note that according to Annex VI, state law protections must be at least equal to those of the U.S. Constitution, including but not limited to the Fourth Amendment. The EDPB invites the Commission to further assess the element of state law protection in the future reviews.

3.1.2 Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

83. The EDPB duly notes that requesting access to data for law enforcement purposes can, in general, be considered to pursue a legitimate objective. However, at the same time, such interferences are only acceptable when they are necessary and proportionate.⁸⁴
84. According to the settled case-law of the CJEU, the principle of proportionality requires that the legislative measures introducing interferences with the rights to private life and to the protection of personal data “be appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives”⁸⁵. Therefore, the assessment of necessity and proportionality is, in principle, always done in relation to a specific measure envisaged by legislation.
85. The U.S. authorities specify in Annex VI that federal prosecutors and federal investigative agents are able to gain access to documents and other record information from organisations through “several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas, and search warrants” and may acquire other communications “pursuant to federal criminal wiretap and

⁸¹ 31 U.S.C. § 5318; 31 C.F.R. Chapter X

⁸² 15 U.S.C. § 1681b

⁸³ 12 U.S.C. §§ 3401-3423

⁸⁴ See Judgment of the Court of Justice of 6 October 2020 in joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, ECLI:EU:C:2020:791 (hereinafter, ‘CJEU La Quadrature du Net judgment’), paragraph 140. See also EDPS, [Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit](#), 11 April 2017 and EDPS [Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data](#), 19 December 2019.

⁸⁵ See Judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland, ECLI:EU:C:2014:238 (hereinafter: ‘CJEU Digital Rights Ireland judgment’), paragraph 46 and case-law cited therein.

pen register authorities”⁸⁶. In addition, agencies with civil and regulatory responsibilities may issue subpoenas to organisations for “business records, electronically stored information, or other tangible items”⁸⁷. The processes themselves are also explained in recitals 90-93 of the Draft Decision. The EDPB notes in this regard a positive development referred to in the Draft Decision in the U.S. jurisprudence regarding the electronically stored information⁸⁸.

86. Annex VI furthermore specifies that these legal proceedings are non-discriminatory and used in general to obtain information from ‘corporations’ in the U.S., irrespective of whether they are certified or not within the U.S.-EU Data Privacy Framework, and “without regard to the nationality or place of residence of the data subject”.
87. In addition, Annex VI contains findings regarding the safeguards under the Fourth Amendment of the U.S. Constitution, according to which searches and seizures by law enforcement authorities principally require a court-ordered warrant upon a showing of probable cause and particularity requirements and refers to the fact that in exceptional cases where the warrant requirement does not apply, law enforcement is subject to a reasonableness test under the Fourth Amendment⁸⁹. A person subject to a search or whose property is subject to a search may move to suppress evidence obtained or derived from an unlawful search if that evidence is introduced against that person during a criminal trial⁹⁰.
88. In conclusion, the EDPB notes that the system of investigative tools used to obtain commercial data and other record information from corporations in the U.S. for criminal law enforcement or public interest purposes – including the access limitations and safeguards – provides a comprehensive but also a complex system of measures, reflecting, among other things, the federal nature of the U.S government.
89. Thus, the system of law enforcement investigative measures in the U.S could be considered as generally meeting the requirements of necessity and proportionality in relation to the fundamental rights to private life and data protection.

3.1.3 An independent oversight mechanism should exist

90. The EDPB duly notes the fact that most of the procedures described in the Draft Decision and Annex VI presuppose the involvement of a court’s decision before the authorities obtain access to data (e.g. court orders for pen register and trap and races⁹¹, court orders for surveillance pursuant to the Federal Wiretap Law⁹², search warrants – Federal Rules of Criminal Procedure, Rule 41⁹³). However, it seems that not all of them require the a priori involvement of a court. For instance, civil and regulatory authorities “may issue subpoenas”⁹⁴. In these cases however, there is the possibility of an ex post

⁸⁶ Draft Decision, Annex VI, p. 2.

⁸⁷ Draft Decision, Annex VI, p. 4.

⁸⁸ See Draft Decision, footnote 146. In a 2018 judgment, the U.S. Supreme Court confirmed that a search warrant or warrant exception is also required for law enforcement authorities to access historical cell site location records, that provide a comprehensive overview of a user’s movements and that the user can have a reasonable expectation of privacy with respect to such information (*Timothy Ivory Carpenter v. United States of America*, No. 16-402, 585 U.S. (2018)).

⁸⁹ See Draft Decision, Annex VI, p. 2.

⁹⁰ See Draft Decision, recital 90.

⁹¹ See Draft Decision, recital 92.

⁹² See Draft Decision, Annex VI, p 3.

⁹³ See Draft Decision, recital 90 and Annex VI, p 3.

⁹⁴ See Draft Decision, Annex VI, p. 4 as well as recital 91.

judicial control of the reasonableness of the subpoena, as “a recipient of an administrative subpoena may challenge the enforcement of that subpoena in court”⁹⁵.

91. In addition, the Draft Decision describes the oversight of the federal criminal law enforcement agencies by various bodies, from the inner control by the Privacy and Civil Liberties Officers to the external control carried out by the Inspector General and specific Committees in the U.S. Congress⁹⁶. The European Commission provides nuanced and detailed information, and generally reaches comprehensible conclusions. Therefore, the EDPB refrains from reproducing the factual finding and assessments in this opinion.
92. Based on the available information, the EDPB notes that, with regard to access by law enforcement authorities to data held by companies in the U.S., a fairly robust independent oversight mechanism is in place.

3.1.4 Effective remedies need to be available to the individual

93. According to the jurisprudence of the CJEU, an individual must have an effective remedy to satisfy their rights when they consider that they are not or have not been respected. The CJEU explained in Schrems I that “legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article.”⁹⁷
94. The Draft Decision⁹⁸ and its Annex VI contain further information with regard to possible remedies stemming from statutory law, which would be available to individuals when public authorities unlawfully obtain access to their data.
95. In this regard, according to the Commission⁹⁹, 5 U.S.C. § 702 (Administrative Procedure Act (APA)), provides that a person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof.
96. Furthermore, the Stored Communications Act (SCA) (enacted as title II of the Electronic Communications Privacy Act) provides that, any person aggrieved by any violation of that chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate¹⁰⁰. In addition, any person who is aggrieved by any willful violation of that chapter or of chapter 119 may commence an action in United States District Court against the United States to recover money damages¹⁰¹.

⁹⁵ See Draft Decision, Annex VI, p. 4 as well as recital 91.

⁹⁶ See Draft Decision, Recitals 103-106.

⁹⁷ CJEU Schrems I judgment, paragraph 95.

⁹⁸ See Draft Decision, recitals 107 to 112.

⁹⁹ See Draft Decision, recital 109.

¹⁰⁰ 18 U.S.C. § 2707

¹⁰¹ 18 U.S.C. § 2712

97. Moreover, the Draft Decision also contains information on the right to obtain access to federal agency records under the Freedom of Information Act (FOIA)¹⁰² and several other statutes which afford individuals the right to bring suit against a U.S. public authority or official with respect to the processing of their personal data, such as the, Wiretap Act, the Computer Fraud and Abuse Act, the Federal Torts Claim Act, the Right to Financial Privacy Act, and the Fair Credit Reporting Act¹⁰³.
98. The EDPB therefore welcomes the clarifications provided by the Commission as to the number of legal avenues for redress for individuals to rely on. The EDPB also invites the Commission to further clarify whether these remedies allow the data subject to ‘have access to personal data relating to him, or to obtain the rectification or erasure of such data’ as required by the CJEU.

3.1.5 Further use of the information collected

3.1.5.1 Further use of transferred data accessed by LEA within the US

99. The EDPB positively notes that the Draft Decision assesses the further use of data accessed by law enforcement authorities within the U.S. However, the EDPB regrets that only one example of the grounds on which the information can be further disseminated is given¹⁰⁴. In that regard, the EDPB recommends the Commission to include further clarification in the Draft Decision on the principles and safeguards applicable on the further use of data, such as those included in the Privacy Act (5 U.S.C. 552a)¹⁰⁵.

3.1.5.2 Onward transfers outside the U.S.

100. The EDPB further notes that the European Commission has also referred to onward transfers from the law enforcement authorities in the U.S to authorities in third countries, but again only with regard to the Attorney General Guidelines for Domestic FBI Operations AGG-DOM¹⁰⁶. The EDPB considers that such information and assessment are essential in order to allow a comprehensive assessment of the level of protection afforded by the U.S. legislative framework and practices in relation to international disclosure and further use. Given that the Commission has given only one, limited, example regarding the issue of onward transfers outside the U.S. as a whole, the EDPB invites the Commission to further clarify the applicable rules and safeguards for onward transfers, further use and disclosure of personal information, collected for law enforcement purposes in the U.S. and subsequently transferred to third countries, including via international agreements.

3.2 Access and use for national security purposes

101. As a general remark, the EDPB acknowledges that States are granted a broad margin of appreciation in matters of national security, which is also recognised by the ECtHR. The EDPB also recalls that, as underlined in its updated recommendations on the European essential guarantees for surveillances measures¹⁰⁷, Article 6(3) Treaty on European Union establishes that the fundamental rights enshrined in the ECHR constitute general principles of EU law. However, as the CJEU recalls in its jurisprudence, the latter does not constitute, as long as the EU has not acceded to it, a legal instrument which has

¹⁰² See Draft Decision, recital 111.

¹⁰³ See Draft Decision, recital 112.

¹⁰⁴ See Draft Decision, recital 102.

¹⁰⁵ See Attorney General Guidelines for Domestic FBI Operations (AGG-DOM), page 36, p. B (1)(g)

¹⁰⁶ See Draft Decision, recital 102.

¹⁰⁷ See EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

been formally incorporated into EU law¹⁰⁸. Thus, the level of protection of fundamental rights required by Article 45 GDPR must be determined on the basis of the provisions of that regulation, read in the light of the fundamental rights enshrined in the EU Charter. This being said, according to Article 52(3) EU Charter, the rights contained therein that correspond to rights guaranteed by the ECHR are to have the same meaning and scope as those laid down by the ECHR. Consequently, as recalled by the CJEU, the jurisprudence of the ECtHR concerning rights that are also foreseen in the EU Charter must be taken into account, as a minimum threshold of protection to interpret corresponding rights in the EU Charter¹⁰⁹. According to the last sentence of Article 52(3) EU Charter, however, “[t]his provision shall not prevent Union law providing more extensive protection.”

102. Therefore, in the following assessment, the EDPR has taken into account the jurisprudence of the ECtHR, to the extent that the EU Charter, as interpreted by the CJEU, does not provide for a higher level of protection which prescribes other requirements than the ECtHR case-law.
103. Several legal instruments provide for the possibility to collect and further access and process data for U.S. Intelligence agencies in the U.S. legal framework.
104. As recalled by the European Commission in its Draft Decision, “U.S. intelligence agencies may seek access to personal data that has been transferred to organisations located in the United States for national security purposes only as authorised by statute, specifically under the Foreign Intelligence Surveillance Act (FISA) or and statutory provisions authorising access through National Security Letters (NSL)”¹¹⁰. “U.S. intelligence agencies also have possibilities to collect personal data outside the United States, which may include personal data in transit between the Union and the United States” under the Executive Order 12333 (EO 12333)¹¹¹.
105. With respect to the specific data collection regimes, in particular Section 702 FISA and EO 12333, EO 14086 now provides for new rules to enhance safeguards for the United States Signals Intelligence Activities. These general rules apply horizontally and “must be further implemented through agency policies and procedures that transpose them into concrete directions for day-to-day operations”¹¹². The EO 14086 has mostly replaced the previous Presidential Policy Directive 28 ('PPD-28')¹¹³.
106. In order to assess the legal framework applying to collection, access and further processing of data for national security purposes, it is thus important to examine the specific legal framework governing the collection of data within and outside the U.S., i.e. Section 702 FISA and EO 12333, which, as such, have not changed since the previous review of the Privacy Shield, taking into account the fact that the new Executive Order 14086 provides safeguards to be implemented also in the context of collection of data on the ground of specific texts such as Section 702 FISA and EO 12333.

¹⁰⁸ See CJEU Schrems II judgment, para. 98.

¹⁰⁹ See CJEU La Quadrature du Net judgment, para. 124.

¹¹⁰ See Draft Decision, recital 115.

¹¹¹ See Draft Decision, recital 117.

¹¹² See Draft Decision, recital 120.

¹¹³ This Executive Order revokes PPD-28 except for sections 3 and 6 of that directive and the classified annex to that directive, which remain in effect. See presidential national security memorandum of 7 October 2022.

3.2.1 Guarantee A - Processing should be in accordance with the law and based on clear, precise and accessible rules

107. For its assessment of the general setup of data collection for the purpose of national security, the EDPB wishes to recall the first of the four so called “European essential guarantees”, according to which ‘processing should be based on clear, precise and accessible rules’¹¹⁴.
108. In accordance with the settled case law of the CJEU, any limitation to the right to the protection of personal data must be provided for by law and the legal basis which permits the interference with such a right must itself define the scope of the limitation to the exercise of the right concerned¹¹⁵. The Court also recalled that “legislation must be legally binding under domestic law”¹¹⁶. In this regard, the ECtHR case-law clarifies that the term ‘law’ should be understood in its substantive sense, not its formal one. It may include enactments of lower ranking statutes and regulatory measures taken by professional regulatory bodies under independent rule-making powers delegated to them by Parliament and even unwritten law. To be ‘law’, a norm must at least be adequately accessible and formulated with sufficient precision¹¹⁷.
109. The degree of precision required must be measured in relation to the extent of the limitation of the right¹¹⁸. Furthermore, as regards ‘foreseeability’ of the law, the ECtHR recalled in *Zakharov* that in the context of secret measures of surveillance, such as the interception of communications, “foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly”. However, clear and detailed rules on secret surveillance measures are essential to prevent the risks of arbitrariness where a power vested in the executive is exercised in secret. “The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures”¹¹⁹.
110. In addition, the CJEU clarified that the assessment of the applicable third country law should focus on whether it can be invoked and relied on by individuals before a court. The rights granted to data subjects should notably be actionable and individuals have to be provided with enforceable rights against public authorities¹²⁰, which was not the case in the context of the previous PPD-28. The EO 14086, which, the EDPB understands, is deemed to have the same legal effect within the US legal order as PPD-28 (i.e. binding on the executive), now provides for actionable entitlements against public authorities. A detailed assessment of the new enforceable rights of the data subjects is provided in the section on redress.
111. Recitals 114-152 of the Draft Decision and Annex VII provide a summary of some aspects of the governing legal framework, the collection limitations, the retention and dissemination limitations, compliance and oversight, transparency and redress. The U.S. legal system for intelligence activities

¹¹⁴ Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020. See §175 and §180 Schrems II and Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, § 139 and the case-law cited.

¹¹⁵ See CJEU Schrems II judgment, paragraphs 174-175 and the case-law cited. See also, as regards access by public authorities of Member States, Case C-623/17 Privacy International ECLI:EU:C:2020:790 (hereinafter, ‘CJEU Privacy International judgment’), paragraph 65; and CJEU La Quadrature du Net judgment, paragraph 175.

¹¹⁶ CJEU Privacy International judgment, paragraph 68.

¹¹⁷ ECtHR, *Sunday Times v UK (No 1)*, 26 April 1979, CE:ECHR:1979:0426JUD000653874 (hereinafter, ‘ECtHR Sunday Times v UK No 1 judgment’), para 49.

¹¹⁸ ECtHR *Sunday Times v UK No 1 judgment*, para 49.

¹¹⁹ ECtHR, *Zakharov v. Russia*, 4 December 2015 (hereinafter, ‘ECtHR Zakharov judgment’), paragraph 229.

¹²⁰ CJEU Schrems II judgment, paragraph 181.

consists of a number of different documents including individual agencies reports, policies and procedures. In that regard, the EDPB evaluation is focused on a limited number of issues that it considers crucial.

112. According to recitals 115 to 119 of the Draft Decision, access to transferred personal data by US national security authorities may only take place under FISA, under other statutory provisions (12 U.S.C. §3414, 15 U.S.C. § 1681u-1681v and 18 U.S.C. § 2709) or, in connection with personal data in transit, on the basis of EO 12333. It stems from recitals 116 and 118 of the Draft Decision that the Commission focuses its assessment, in connection with access to personal data by US national security authorities, on sections 105, 302, 402, 501 and 702 FISA (foreign intelligence activities targeting non-US persons located outside the US) and EO 12333 (foreign intelligence activities on personal data in transit), as being the most relevant. The EDPB opinion is therefore limited to the assessment of these provisions made by the Commission, taking into account the limitations and safeguards set out in EO 14086¹²¹.
113. In this respect, it is to be noted that all legal instruments mentioned in the Draft Decision are accessible for the general public (in and outside of the U.S.) and available online. Furthermore, the requirements laid down in the EO are binding on the entire Intelligence Community¹²² and apply in a cross-cutting way to all foreign intelligence purpose activities.
114. The concept of 'signals intelligence' is not defined in the EO 14086. The latter refers to the definitions set out in the EO 12333 for establishing the scope of foreign intelligence and counterintelligence, which are defined broadly. In this regard, even if it has been argued that since the introduction of FISA, EO 12333 can only be used for the collection of data outside the U.S. territory, the EDPB recalls that EO 12333 itself, which remains intact, lacks of sufficient details regarding its geographical scope, the extent to which data can be collected, retained or further disseminated, or on the nature of offences that may give rise to surveillance or the kind of information that may be collected or used. In principle, all foreign intelligence data collection within the scope of EO 12333 can take place at the discretion of the U.S. President.¹²³ However, in the understanding of the EDPB, the main purpose of the EO 14086 is to prescribe the limits for the collection and the processing of personal data in the context of foreign intelligence, no matter which surveillance programme is used and where data is obtained from. It is therefore the understanding of the EDPB that the additional safeguards provided for under EO 14086 also apply in the context of surveillance programmes applicable to personal data in transit taking place under EO 12333¹²⁴.
115. In this respect, the EO 14086 lists 12 legitimate objectives that should be pursued when conducting signals intelligence collection and 5 objectives for which signals intelligence collection must not be conducted¹²⁵, as well as 6 legitimate objectives for the use of data collected in bulk¹²⁶. While some of them are quite detailed (e.g. 'rescue of hostages'), some others are more general (e.g. 'global security'). The EO 14086 sets out also a list of prohibited objectives, which includes notably the

¹²¹ This Executive Order revokes PPD-28 except for sections 3 and 6 of that directive and the classified annex to that directive, which remain in effect. See [presidential national security memorandum of 7 October 2022](#)

¹²² See Draft Decision, recital 120.

¹²³ Under Article II of the U.S. Constitution, responsibility ensuring national security including in particular gathering foreign intelligence falls within the President's authority as Commander in Chief of the armed forces.

¹²⁴ See Draft Decision, recital 134.

¹²⁵ See Executive Order 14086 ('EO 14086'), section 2, (b), (ii), A, 1 to 5.

¹²⁶ See Draft Decision, recital 134 and EO 14086, section 2(c)(ii).

suppression or restriction of 'legitimate privacy interests'¹²⁷. The EO 14086 also provides for the possibility for the President of the United States to add other objectives to the list for which collection is allowed, which could, upon decision of the President, not be released to the public if the President considers that doing so would pose a risk to the national security of the United States¹²⁸. Such updates may only be authorised 'in light of new national security imperatives'.

116. The objectives cannot by themselves be relied upon by intelligence agencies to justify signals intelligence collection but must be further substantiated, for operational purposes, into more concrete priorities for which signals intelligence may be collected. The EO 14086 details the procedure for the validation of the priorities for which signals intelligence may be collected¹²⁹. The EDPB understands that the process to define the validated intelligence priorities in principle relies on the Director of the Intelligence Community and acknowledges that it should as a rule involve the assessment of the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO), with which the Director can disagree, in which case it "shall include the CLPO's assessment and the Director's views when presenting the National Intelligence Priorities Framework (NIPF) to the President"¹³⁰.
117. However, the EDPB also notes that according to the definition of "*validated intelligence priority*", such priorities mean for "*most United States signals intelligence collection activities*"¹³¹ a priority validated under section 2(b)(iii) of the EO (described in the previous paragraph). The process of validation can in some cases differ from this process in "*narrow circumstances*", in which case, the President or the head of an element of the Intelligence Community may set a priority, "*to the extent feasible*" in accordance with the criteria set by the same section 2(b)(iii)(A)(1)-(3), which includes the requirement for appropriate consideration for the privacy and civil liberties of all persons, but without the involvement of the CLPO.
118. The EO 14086 in addition underlines that 'signals intelligence collection activities shall be as tailored as feasible' to advance a validated intelligence priority, and that 'the Intelligence Community shall consider the availability, feasibility, and appropriateness of other less intrusive sources' and provides general necessity and proportionality requirements¹³².
119. Furthermore, according to Section 5(h), EO 14086 creates an entitlement to submit qualifying complaints to the CLPO and to obtain review of the CLPO's decisions by the Data Protection Review Court in accordance with the redress mechanism established in section 3 of that Order.
120. The text of FISA appears to be clearer and more precise than EO 12333 on the kind of intelligence operations that can be mandated. FISA and EO 12333 now have to be applied in the light of EO 14086 and in particular taking into account inter alia the principles of necessity and proportionality.
121. The requirements laid down in the EO 14086 must be further implemented through agency policies and procedures that transpose them into concrete directions for day-to-day operations. In this respect, EO 14086 provides U.S. intelligence agencies with a maximum of one year to update their existing policies and procedures (i.e. by 7 October 2023) to bring them in line with the EO's requirements. Such updated policies and procedures have to be developed in consultation with the Attorney General, the

¹²⁷ See EO 14086, Section 2(b)(ii)(A)(2).

¹²⁸ See EO 14086, Section 2(b)(i)(B).

¹²⁹ See Draft Decision, recital 129.

¹³⁰ See EO 14086, section 2(b)(iii)(B).

¹³¹ See EO 14086, Section 4, (n)

¹³² See EO 14086, Section 2(c)(i) (A) and (B).

CLPO and the Privacy and Civil Liberties Oversight Board (PCLOB) and be made publicly available to the maximum extent possible¹³³.

122. The EDPB would welcome that not only the entry into force but also the adoption of the decision are conditional upon *inter alia* the adoption of updated policies and procedures to implement EO 14086 by all US intelligence agencies. The EDPB recommends the Commission to assess these updated policies and procedures and share this assessment with the EDPB.
123. Finally, in relation to the retention of the transferred data once collected for national security purposes, the EDPB notes that the EO 14086 ensures that the rules applicable to personal data of US persons are also applicable to non-US persons' personal data¹³⁴. From the Draft Decision, it appears that these rules are provided for in section 309 of the Intelligence Authorization Act for Fiscal Year 2015¹³⁵, which establishes a maximum retention period of 5 years in principle of any non-public telephone or electronic communication acquired without the consent of the person. The EDPB recommends in this regard that the Commission provide more clarity as to its assessment of the retention rules applicable to personal data of US persons in the decision.

3.2.2 Guarantee B - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated

3.2.2.1 *Horizontal safeguards provided by the new Executive Order 14086 – Necessity and proportionality*

124. The new EO 14086 which generally replaces PPD-28, aims at providing rules to enhance safeguards for United States Signals Intelligence Activities, to be further implemented by the Intelligence Community elements in their internal policies and procedures.
125. EO 14086 introduces two new requirements under US law which echo the requirements recalled by the CJEU in its Schrems II judgment, namely that signals intelligence activities shall be conducted only as far as necessary to advance a validated intelligence priority collection and only to the extent and in a manner that is proportionate to the validated intelligence priority¹³⁶.
126. It is the understanding of the EDPB that these elements have been included to reflect the principles of necessity and proportionality foreseen under EU law and in the CJEU and ECHR case-law which aim at ensuring that collection and processing of data should be limited to what is necessary and proportionate.
127. In this regard the EDPB recalls the process foreseen for the validation of intelligence priorities as well as the possible derogation (see paragraphs 116, 117).
128. Furthermore, the EDPB notes that these principles of necessity and proportionality provided in the EO will have to be operationalized and implemented, within one year, in the policies and procedures of each element of the Intelligence Community¹³⁷.

¹³³ See EO 14086, Section 2(c)(iv)(B) and (C).

¹³⁴ Draft Decision, recital 150.

¹³⁵ Draft Decision, footnote 272.

¹³⁶ See EO 14086, Section 2, (a), (ii), A and B.

¹³⁷ See EO 14086, Section 2, (c), (iv), B

3.2.2.2 Specific safeguards for the collection of signals intelligence

129. The EDPB also notes that EO 14086 provides for limitations regarding the objectives for which personal data can and cannot be collected, in the context of collection of signals intelligence¹³⁸.
130. The EDPB welcomes that the EO provides that targeted collection should be prioritized over bulk collection¹³⁹. In the context of collection of signals intelligence, the EO provides for a list of 12 objectives for which data can be collected, which have to be further substantiated into intelligence priorities (see paragraph 117), as well as a list of 5 objectives for which signals intelligence collection activities shall not be conducted¹⁴⁰. In principle these provisions constitute a guarantee to ensure the necessity of the collection of data.
131. Yet, the EDPB recalls that EO 14086, also provides for the possibility for the President of the United States to add other objectives to the list (see paragraphs 114, 115).¹⁴¹

3.2.2.3 Specific safeguards for bulk collection

132. The CJEU underlined in its Schrems I judgment that the “*protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary*”¹⁴² and ruled that “*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter*”.
133. In the Schrems II case¹⁴³, with regards to its analysis of bulk collection in relation to the correlated reading of EO 12 333 and PPD-28, and in particular points 183 to 185, the Court stressed, as recalled above, that the possibility of bulk collection, « *which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data.* ».
134. The EDPB thus notes that the CJEU did not exclude, by principle, bulk collection, but considered in its Schrems II decision that for such bulk collection to take place lawfully, sufficiently clear and precise limits must be in place to delimit the scope of such bulk collection.
135. The EDPB also recognizes that while replacing the PPD-28, the EO 14086 provides for new safeguards and limits to the collection and use of data collected outside the U.S., as the limitations of FISA or other more specific U.S. laws do not apply.
136. With regards to bulk collection of data, the EDPB takes note that the EO 14086 provides that bulk collection continues to be permitted. Indeed, the EDPB underlines that the definition of bulk collection remains the same as in the previous PPD-28: “*signals intelligence collected in ‘bulk’ means the authorised collection of large quantities of signals intelligence data which, due to technical or*

¹³⁸ See EO 14086, section 2, (b), (i), A, 1 to 12

¹³⁹ See EO 14086, section 2, (c), (ii), A

¹⁴⁰ See EO 14086, section 2, (b), (iii), A, 1 to 5

¹⁴¹ See EO 14086, section 2, (b), (i), B

¹⁴² CJEU Schrems I judgment, para 92.

¹⁴³ See CJEU Schrems II judgment.

*operational considerations, is acquired without the use of discriminants (for example, without the use of specific identifiers or selection terms.)*¹⁴⁴.

137. Since the Schrems II ruling, the Court did not detail precisely the safeguards required for bulk collection to take place. However, the EDPB recalls that the ECHR has issued important decisions concerning bulk collection and the relevant safeguards in this context.
138. The EDPB recalls that bulk collection, by allowing for the collection of large quantities of data without discriminant presents higher risks for the individuals¹⁴⁵ than targeted collection and thus requires additional safeguards to be adduced.
139. The EDPB also notes that the CJEU has developed further case law concerning retention of traffic and location data, and subsequent access to these data retained by telecommunications operators, including for national security purposes, which, although they cannot be deemed directly applicable in this context, to some extent could be relevant in the context of the present assessment of bulk collection in the context of EO 12333.

1) Purpose limitation

140. The EO provides that bulk collection should take place only following a determination that « *the information necessary to advance a validated intelligence priority cannot reasonably be obtained by targeted collection* »¹⁴⁶, and that « *the element of the Intelligence Community shall apply reasonable methods and technical measures in order to limit the data collected to only what is necessary to advance a validated intelligence priority, while minimizing the collection of non-pertinent information* »¹⁴⁷. In addition to these safeguards, the EDPB also recognizes that the use of data collected in bulk shall be used in pursuit of one or more of the six objectives listed¹⁴⁸. The EDPB further stresses that while these objectives are more detailed than those which were provided in the previous PPD-28, generally replaced by EO 14086, the scale of such collection possibilities remains potentially broad, i.e. encompassing large volumes of data.
141. The EDPB here as well recalls that EO 14086, also provides for the possibility for the President of the United States to add other objectives to the list (see paragraph 115)¹⁴⁹.

2) Prior independent authorisation

142. The EDPB stresses that the ECtHR dedicates a significant importance to prior independent authorization in the context of bulk collection of data for national security purposes. Indeed the Court ruled in particular that “*in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to “end-to-end safeguards”, meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent*

¹⁴⁴ See EO 14086, Section 4, (b)

¹⁴⁵ See for instance ECtHR (Grand Chamber), Big Brother Watch and others v. The United Kingdom, 25 May 2021 (hereinafter, ‘ECtHR Big Brother Watch judgment’), recital 363, where the Court indicates that it “*is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content*”.

¹⁴⁶ EO 14086, Section 2(c)(ii)(A).

¹⁴⁷ EO 14086, Section 2(c)(ii)(A).

¹⁴⁸ EO 14086, Section 2(c)(ii)(B).

¹⁴⁹ See EO 14086, Section 2(c)(ii)(C).

*authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime.*¹⁵⁰

143. The EDPB also notes the following paragraph of this judgment in Grand Chamber, where the Strasbourg Court further highlights that it “*agrees with the Chamber that while judicial authorisation is an important safeguard against arbitrariness*” it is not a “*necessary requirement*” (see paragraphs 318-320 of the Chamber judgment). Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive¹⁵¹.
144. In this context, the EDPB notes that the EO does not provide for such independent prior authorization for bulk collection, and that this is not foreseen as well under EO 12333 (see section below on EO 12333).

3) *Retention rules*

145. The EDPB recalls that another important set of safeguards are the rules for the duration of the collection and retention of data. In this respect, the ECtHR stressed that “*domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed*”¹⁵² as these safeguards “*are equally relevant to bulk interception*.¹⁵³
146. In this regard, it is the understanding of the EDPB that the EO provides for rules concerning the retention of data for personal data collected through signals intelligence, including in bulk¹⁵⁴. The EDPB notes that, according to Section 2(c)(iii)(A) of EO 14086, each element of the Intelligence Community that handles personal information collected through signals intelligence shall establish and apply policies and procedures designed to minimize the dissemination and retention of personal information collected through signals intelligence. However, these rules do not provide for a specific retention period but rather refer in general to the same applicable rules for the retention of data concerning US persons and to situations where no final retention determination has been made. The EDPB is thus concerned that these retention periods, as for targeted collection (see paragraph 122), are not clearly defined in this EO with regards to data collected in bulk. It calls on the Commission to share its assessment on the necessity and proportionality of the retention periods applicable to US persons and the available information concerning retention periods in practice where no final retention determination has been made under US law, as in its current state, the Draft Decision merely recalls this general rule in a single short paragraph¹⁵⁵ and a footnote¹⁵⁶ which does not allow to determine whether these retention periods are necessary and proportionate. Since, as underlined by the ECtHR, this is a crucial safeguard for data subjects to be able to exercise their rights in a context where a particularly intrusive measure is taken to collect their data in the first place, the EDPB calls on the

¹⁵⁰ See ECtHR Big Brother Watch judgment, para. 350.

¹⁵¹ See ECtHR Big Brother Watch judgment, para. 351.

¹⁵² See ECtHR Big Brother Watch judgment, para. 348.

¹⁵³ See ECtHR Big Brother Watch judgment, para. 348.

¹⁵⁴ See EO 14086, section 2, (c), (iii), A, (2)(a)-(c).

¹⁵⁵ See Draft Decision, para. 150.

¹⁵⁶ See Draft Decision, footnote 271.

European Commission to provide further clarifications concerning the different retention periods in practice.

4) Safeguards concerning “dissemination”

147. Also, the EDPB recalls that to ensure the effectivity of necessity and proportionality and the purpose limitation principle, the ECtHR also recognized the importance of rules provided by law concerning the further dissemination of the data collected, including in context of bulk collection¹⁵⁷.
148. Section 2(c)(iii)(A)(1)(c) of EO 14086 provides that information about non-U.S. persons that was collected through signals intelligence activities may only be disseminated if an authorized and appropriately trained individual has a reasonable belief that the personal information will be appropriately protected and that the recipient has a need to know the information.
149. Taking this into account, the EDPB understands that the provisions concerning dissemination under the EO 14086 do not provide neither for an express prohibition of dissemination for other purposes than national security purposes when dissemination to US competent authorities is concerned¹⁵⁸. The EDPB calls on the Commission to further clarify the applicable rules and safeguards in this case.
150. The EDPB is therefore concerned that data acquired by the competent Intelligence Community authorities could then be disseminated to US competent authorities for the purpose of combating crime, including serious crimes, in the context of criminal investigations, thereby providing law enforcement authorities, without any further specific restrictions, with a possibility to obtain data that they would have been prohibited from collecting directly and calls on the Commission to further assess this point.
151. In the specific context of onward transfers (dissemination to recipients outside the United States Government, including to a foreign government or international organization¹⁵⁹), the EDPB recalls that it is of the view that the protection afforded to data should also be maintained in the context of onward transfers including in the field of national security¹⁶⁰.
152. In this respect, the EO provides for some safeguards, namely the requirement to take due account of the purpose of the dissemination – although without expressly requiring that the purpose of dissemination should also be for the protection of national security – the nature and the extent of the personal information being disseminated and the potential harmful impact on the person or persons concerned before disseminating the data.
153. While the EDPB acknowledges that some of these safeguards, in particular the account to be given to the “*potential for harmful impact*”¹⁶¹ on the data subject(s) concerned, reflect some requirements of the ECHR, it also stresses that the Strasbourg Court furthermore requires that a legally binding obligation “*to analyse and determine whether the foreign recipient of intelligence offers an acceptable minimum level of safeguards*”¹⁶², which the EDPB does not expressly find in the provisions of the EO

¹⁵⁷ See ECtHR Big Brother Watch judgment, para. 348.

¹⁵⁸ See EO 14086, Sec 2.(c)(iii)(A)(1).

¹⁵⁹ See EO 14086, Sec 2.(c)(iii)(A)(1), (d) in particular.

¹⁶⁰ See for instance EDPB Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom. Adopted on 13 April 2021, sections 4.3.2.1 and 4.3.2.2.

¹⁶¹ See EO 14086, Sec 2.(c)(iii)(A)(1), (d)

¹⁶² See ECtHR (Grand Chamber), Case of Centrum För Rättvisa V. Sweden, 25 May 2021, para 326.

relating to dissemination to foreign recipients. The EDPB invites therefore the Commission to further assess this element.

154. The EDPB also notes that the European Commission did not consider, as part of its adequacy assessment, the existence of international agreements concluded with third countries or international organisations that may provide for specific provisions for the international transfer of personal data by intelligence services to third countries. The EDPB considers that the conclusion of bilateral or multilateral agreements with third countries for the purposes of intelligence cooperation are likely to affect the data protection legal framework as assessed.
155. The EDPB therefore invites the European Commission to clarify whether such agreements exist, under which conditions they may be concluded and assess whether the provisions of international agreements may affect the level of protection afforded to personal data transferred from the EEA by the legislative framework and practices in relation to onward transfers for national security purposes.

5) Temporary bulk collection to support the initial technical phase of targeted collection

156. The EDPB recalls that, in the context of the last Joint Review of the Privacy Shield, discussions mainly focused on the interpretation and application of the additional ground (situation/scenario) for bulk collection foreseen by the first sentence of footnote 5 of Section 2 PPD28-, which provided that "*The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection.*" The U.S. authorities explained at the time the meaning of "*signals intelligence data that is temporarily acquired to facilitate targeted collection*". The EDPB understood from these discussions that this footnote meant that data may be collected in bulk - and regardless of the six purposes foreseen - if collected temporarily, with a view to establishing an identifier for a defined target. This would thus be an additional ground to collect data in bulk, and in this case only the general principles of Section 1 of PPD-28 would have still applied. As recalled above, in the Schrems II ruling, the CJEU considered that the combined EO 12333 and PPD-28 with regards to bulk collection did not "*delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data*"¹⁶³.
157. The EDPB notes that a derogation allowing for such kind of bulk collection is still provided in the EO 14086¹⁶⁴; however, the EDPB welcomes that this derogation has been narrowed compared to PPD-28 and additional safeguards are provided under the EO 14086.
158. The EDPB understands that the new EO 14086 provides for safeguards which remain applicable in the context of this type of temporary technical bulk collection, in particular the general principles of necessity and proportionality in relation to the validated intelligence priority when data are acquired without discriminants before targeted collection takes place (Section 2(a)-(b), Section 2(c)(i) EO 14086). It is also the understanding of the EDPB that such bulk collection supporting a subsequent targeted signals intelligence collection is also subject to the additional safeguards provided from subsection (2)(c)(iii) onwards¹⁶⁵.
159. However, the EDPB also recalls – see above paragraph 117 – that the definition of "*validated intelligence priority*" provides for a derogatory procedure which would not involve the CLPO of the Office of the Director of National Intelligence.

¹⁶³ CJEU Schrems II judgment, paragraph 183.

¹⁶⁴ See EO 14086, section 2 (c), (ii), D and Draft Decision, footnote 226.

¹⁶⁵ See previous sections for further elements on these provisions.

160. However, the EDPB still notes that the safeguards of the subsection concerning bulk collection do not apply to temporary bulk collection used to support the initial technical phase of targeted signals intelligence collection activity as outlined in Section 2(c)(ii)(D) of EO 14086, which notably means that in this context data collected in bulk can be used for other purposes than those listed under subsection 2 (c)(ii). The EDPB would welcome clarifications in the Draft Decision on the purposes for which data collected in bulk in this context can be used as well as concerning the application of the limitations set out under subsection 2(c)(i) for the collection of signals intelligence in general (namely only for the legitimate objectives listed there) in the context of temporary bulk collection in the Draft Decision.
161. To conclude, the EDPB also stresses that this derogation for temporary bulk collection in view of targeted collection and the remaining safeguards to be applied remains unclear, in particular as to which safeguards of the EO 14086 would apply to which stage (bulk collection, further targeted collection) and calls on the Commission to further assess these elements, and assess these aspects also in practice in the future joint reviews.
162. Furthermore, although the EDPB also further regrets that even if the notion of “temporarily” has been slightly more detailed in the EO than in the PPD-28, in the EDPB’s understanding, it still appears to mean that as long as the target has not been identified, bulk collection could continue. In this regard, the EDPB recalls the necessity to have clear and precise rules and stresses here as well the key safeguard that these rules constitute for data subjects.
163. In conclusion, concerning the safeguards applicable to bulk collection, the EDPB remains concerned that, despite additional safeguards provided under EO 14086, the possibility to collect data in bulk, i.e. without discriminants, is still provided, without key safeguards such as prior authorisation to collect these data - including in the derogatory situation of temporary technical bulk collection -, also taking into account the need for further clarifications and the concerns expressed regarding strict purpose limitation to access the data subsequently, clear and strict data retention rules and stricter safeguards concerning dissemination of data collected in bulk, including in the context of onward transfers.
164. In general, the EDPB stresses that the above-mentioned decision of the ECtHR, once again show the importance of comprehensive supervision by independent supervisory authorities. The EDPB emphasizes that independent oversight at all stages of the process of government access for national security purposes is an important safeguard against arbitrary surveillance measures and thus for the assessment of an adequate level of data protection. The guarantee of independence of the supervisory authorities within the meaning of Article 8(3) of the Charter is intended to ensure effective and reliable monitoring of compliance with the rules on the protection of individuals with regard to the processing of personal data. This applies in particular in circumstances where, due to the nature of secret surveillance, the individual is prevented from seeking review or from taking a direct part in any review proceedings prior or during the execution of the surveillance measure.
165. The EDPB recalls that it is of the opinion that the assessment of adequacy depends on all the circumstances of the case, in particular on the effectiveness of ex post oversight and legal redress as provided for in the legal framework.

3.2.2.4 Legal framework organizing specific collection for national security purposes by the IC elements within and outside the U.S. territory

166. In its Schrems II ruling, the CJEU stressed, in relation to Section 702 FISA that this text “*does not indicate any limitations on the power it confers to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those*

programmes”¹⁶⁶. It led the Court to consider that “in those circumstances (...), that article cannot ensure a level of protection essentially equivalent to that guaranteed by the Charter (...), according to which a legal basis which permits interference with fundamental rights must, in order to satisfy the requirements of the principle of proportionality, itself define the scope of the limitation on the exercise of the right concerned and lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards”¹⁶⁷.

167. In relation to EO 12333, the Court noted that it “does not confer rights which are enforceable against the US authorities in the courts”¹⁶⁸ and also concluded that “in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data”¹⁶⁹, following the analysis of the conditions under which bulk collection could take place under this order, in conjunction with PPD-28.
168. With respect to these specific data collection regimes, EO 14086 now provides for new rules.

3.2.2.4.1 Collection of data for national security purposes under Section 702

169. The EDPB recalls that the findings on FISA 702¹⁷⁰ that “in practice, ‘non-U.S. persons’ also benefit from the access and retention restrictions required by the different agencies’ minimisation and/or targeting procedures due to the cost and difficulty of identifying and removing U.S person information for a large body of data means that typically the entire data set is handled in compliance with the higher U.S data standards” were welcomed in the PCLOB last report.
170. According to those findings, “the programme does not operate by collecting communications in bulk”. The 2014 and 2021 Statistical Transparency Reports issued by the ODNI confirmed this finding. Additionally, according to PCLOB report, “tasked selectors”, such as an e-mail address or a telephone number, are used to target the surveillance.
171. Yet, the EDPB also recalls that, at the same time, in the context of Section 702, it was clarified during the last Review of the Privacy Shield that a “person” to be identified as a target could refer to several individuals using the same identifier, provided that all these individuals would be non-U.S. persons and fulfill the applicable criteria for being targeted. Also the EDPB recalls that during the Third Annual Joint Review of the Privacy Shield in 2019 further clarification in the context of the UPSTREAM program was called upon to exclude that massive and indiscriminate access to personal data of non-U.S. persons take place¹⁷¹.
172. Moreover, the EDPB recalls that the fact that the collection under section 702 FISA is justified by “a significant purpose of the acquisition is to obtain foreign intelligence information” still leaves some uncertainty regarding its purpose limitation and necessity. The EDPB notes however that according to EO 14086, section 2(a)(A) and (B), signals intelligence activities shall be conducted only following a determination that the activities are necessary to advance a validated priority and only to the extent and in a manner that is proportionate to such priority and that it shall be as tailored as feasible to advance the validated priority, taking due account of relevant factors such as the intrusiveness of the

¹⁶⁶ See CJEU Schrems II Judgment, para 180.

¹⁶⁷ See CJEU Schrems II Judgment, para 180.

¹⁶⁸ See CJEU Schrems II Judgment, para 182.

¹⁶⁹ See CJEU Schrems II Judgment, para 183.

¹⁷⁰ See PCLOB Report on the Surveillance program operated pursuant of Section 702 FISA, page 100.

¹⁷¹ See Third Joint Review report, page 17, para 83.

collection, the sensitivity of the data, not disproportionately impact privacy and civil liberties. The EDPB yet expects further clarifications as to how this will be concretely implemented and operationalized, including in the context of the application of FISA Section 702.

173. In this regard, in the absence of direct access to this information by itself, the EDPB called for an independent assessment on the necessity and proportionality of the definition of “targets” and of the concept of “foreign intelligence” under section 702 FISA (including in the context of the UPSTREAM program) following its renewal. The EDPB considers that its previous call for further independent assessment of the process of application of selectors in specific cases (“tasking of selectors”) as well as for further clarification in the context of the UPSTREAM program is relevant. Therefore, taking into account the new EO 14086, the EDPB calls for additional information in order to also assess and monitor how and to which extent the newly introduced principles of necessity and proportionality will be applied in practice in this context and expects that this will also be assessed in the context of future joint reviews.
174. The EDPB welcomes that the fully functional Privacy and Civil Liberties Oversight Board (PCLOB), as an independent oversight agency, has decided to conduct “an Oversight Project to examine the surveillance program that the Executive Branch operates pursuant to Section 702 of the Foreign Intelligence Surveillance Act (FISA), in anticipation of the December 2023 sunset date for Section 702 and the upcoming public and Congressional consideration of its reauthorization”¹⁷². The EDPB also welcomes that the “review covers selected focus areas for investigation, including but not necessarily limited to, U.S. Person queries of information collected under Section 702, and ‘Upstream’ collection conducted pursuant to Section 702”¹⁷³ and “also includes reviewing the program’s past and projected value and efficacy, as well as the adequacy of existing privacy and civil liberties safeguards”¹⁷⁴. The EDPB consequently stresses that access to the findings of the PCLOB in this report on section 702 would be necessary to adequately and comprehensively assess the privacy safeguards provided and applied in the context of this surveillance program.
175. Taking into account the new EO 14086, the EDPB additionally calls for additional information in order to also assess and monitor how and to which extent the newly introduced principles of necessity and proportionality, as well as the other safeguards provided in this text will be applied in practice in this context.

3.2.2.4.2 Collection of data for national security purposes under Executive Order 12333

176. As recognized by the CJEU in its Schrems II ruling, the analysis of the laws of the third country for which adequacy is considered, should not be limited to the laws and practices allowing for surveillance within that country’s physical borders, but should also include an analysis of the legal grounds in that third country’s law which allow it to conduct surveillance outside its territory as far as EU data are concerned. Necessary limitations to governmental access to data should extend to personal data “in transit” to the country, for which adequacy is recognized.
177. The EDPB welcomes the general public report issued by the PCLOB on the Executive Order 12333 and released in April 2021, but notes that this report remains general as most of the findings are classified.

¹⁷² See the [NOTICE OF THE PCLOB OVERSIGHT PROJECT EXAMINING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT \(FISA\)](#)

¹⁷³ See above.

¹⁷⁴ See above.

178. In this context, once again, given the uncertainty and lack of clarity on how EO 12333 used to be applied, and the importance of clarifying how it will be applied in light of the new EO 14086, the EDPB stresses the importance of the awaited PCLOB's reports on this text¹⁷⁵. However, it understands that most of their content is likely to remain classified, so that no further information on the concrete operation of EO 12333 and on its necessity and proportionality would become available neither to the public, nor to the EDPB.
179. The EDPB therefore would particularly welcome the report of the PCLOB on the application of the EO 14086 not being classified but fully accessible once it is completed, including on the parts which would assess how the EO 14086's safeguards will be applied to collection of data under EO 12333. The EDPB also invites the Commission to be specifically attentive to this point in the context of the future joint reviews.
180. In general, with regards to the different legal instruments providing for the possibility to collect and further access and process data for U.S. Intelligence agencies in the U.S. legal framework, the EDPB would welcome clarifications as to their interplay with the new EO 14086 and expects assurances that the previous concerns expressed in the previous opinions of the EDPB in their regards would be resolved by the adoption of these new safeguards.
181. The EDPB also calls on the Commission to be specifically attentive to these aspects in the context of future joint reviews.

3.2.2.4.3 PCLOB report

182. The EDPB welcomes that EO 14086 also provides for the requirement for the PCLOB to produce a report concerning the implementation of the EO. The EDPB stresses that this report should include an assessment of this specific possibility provided by the EO to collect data, for the purposes listed for targeted collection, as well as in bulk, including for technical reasons, in order to better understand the key terms of the EO 14086 and how they are practically understood and applied in the different surveillance programs. This report would also be necessary to assess how the EO will be implemented in the internal procedures and policies of the IC elements.

3.2.3 Guarantee C - Oversight

3.2.3.1 Introduction

183. The U.S. intelligence activities are subject to a multi-layered oversight process. The oversight structure in the U.S. can be divided in internal and external oversight. All intelligence community elements have oversight and compliance officials, which conduct periodic oversight of signals intelligence activities, including Privacy and Civil Liberties Officers and Inspectors General. In addition, there are external oversight bodies, such as the Privacy and Civil Liberties Oversight Board (PCLOB) and the Intelligence Oversight Board.
184. The EDPB recalls that an interference takes place at the time of collection of the data, but also at the time the data is accessed by a public authority for further processing. The ECtHR has specified multiple

¹⁷⁵ The general report on EO 12333 has remained mostly classified - only a short public version has been made public, as well as the report and Recommendations on CIA Counterterrorism Activities Conducted Pursuant to E.O. 12333, as well only partly declassified.

times that any interference with the right to privacy and data protection should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body¹⁷⁶ (e.g. an administrative authority or a parliamentary body).

185. While the ECtHR has expressed its preference for a judge to be responsible to maintain oversight, it did not exclude that another body may be responsible, "*provided that the authority is sufficiently independent from the executive*"¹⁷⁷ and "*of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control*".¹⁷⁸
186. The ECtHR added that "*the manner of appointment and the legal status of the members of the supervisory body*"¹⁷⁹ need to be taken into account when assessing independence.
187. The ECtHR also stated, that it is to examine, whether the supervisory body's activities are open to public scrutiny. For example, this could be accomplished, where the supervision reports annually to the government, respectively the public reports are laid before Parliament and were discussed by Parliament.¹⁸⁰
188. The independent oversight over the implementation of surveillance measures was also taken into account by the CJEU in the Schrems II judgment as that "*[...] the supervisory role of the FISC is thus designed to verify whether those surveillance programmes relate to the objective of acquiring foreign intelligence information, but it does not cover the issue of whether 'individuals are properly targeted to acquire foreign intelligence information'*".¹⁸¹

3.2.3.2 Internal Oversight

3.2.3.2.1 Inspectors General

189. The EDPB recognises that the Inspectors General are entrusted with a wide range of authorisations, necessary to monitor the intelligence activities. In particular, the Inspectors General have access to all information necessary to assess overall compliance of the work of the agencies with the legislation, including but not limited to the laws related to privacy and data protection and can issue subpoenas as well as take an oath from any person in relation to investigation of the Inspectors General.
190. Based on the above, the EDPB considers that the Inspectors General generally have extensive investigatory powers. However, they do not have any binding remedial powers and only issue non-binding recommendations¹⁸².
191. The EDPB recognizes that in principle the Inspectors General shall not be prevented or prohibited from initiating, carrying out, or completing any audit or investigation, or from issuing any subpoena during the course of any audit or investigations.¹⁸³ In this context, the EDPB notes, however, that the

¹⁷⁶ ECtHR, Case of Klass and Others v. Germany, 6 September 1978 (hereinafter, 'ECtHR Klass judgment'), paragraphs 17, 51.

¹⁷⁷ ECtHR Zakharov judgment, paragraph 258; ECtHR, Iordachi and Others v. Moldova, 10 February 2009, paragraphs 40 and 51; ECtHR, Dumitru Popescu v. Romania, 26 April 2007, paragraphs 70-73.

¹⁷⁸ ECtHR Klass judgment, paragraph 56.

¹⁷⁹ ECtHR Zakharov judgment, paragraph 278.

¹⁸⁰ ECtHR Zakharov judgment, paragraph 283; ECtHR, L. v. Norway, 9 June 1990; ECtHR, Kennedy v. the United Kingdom, 18 May 2010, paragraph 166.

¹⁸¹ CJEU Schrems II judgment, paragraph 179.

¹⁸² Draft Decision, recital 105.

¹⁸³ Inspector General Act of 1978, § 3 (a).

Inspectors General are under the authority, direction and control of the respective head of department, who may prohibit them from access to information, undertaking an investigation and among others from issuing any subpoena in cases where the head of department determines that such a prohibition is necessary to preserve national interests. However, the head of department has to inform the responsible committees of the U.S. Congress of the exercise of this authority.¹⁸⁴

192. The EDPB notes that Inspectors General can only be removed by the U.S. President, who must inform to Congress the reasons for such a removal.
193. The EDPB notes that there have not been significant amendments to the internal oversight mechanism since the opinions of the WP 29 and then the EDPB. Therefore, the EDPB follows, in line with the WP 29 Opinion 01/2016¹⁸⁵ that in general sufficient internal oversight mechanisms are in place.

3.2.3.3 External Oversight

194. The EDPB notes that besides the bodies mentioned below, various other bodies within the U.S. government oversee the activities of the U.S. intelligence agencies such as the Intelligence Oversight Board (IOB) or the Congressional committees. The latter can carry out their own investigations and reports.

3.2.3.3.1 Privacy and Civil Liberties Oversight Board (PCLOB)

195. The EDPB recognises the comprehensive supervision role of the PCLOB regarding the new redress mechanism and the implementation of the EO 14086.
196. Firstly, its new functions contain consultation with the Attorney General regarding the appointment of the judges of the DPRC and the special advocates. Secondly, the PCLOB will review the redress process annually, i.e. the processing of qualifying complaints by the redress mechanism. This includes whether the CLPO and the Data Protection Review Court processed qualifying complaints in a timely manner, are obtaining full access to necessary information and operating consistent with the EO 14086 as well as the Intelligence Community's compliance with the determinations made by the CLPO and the DPRC.
197. Furthermore, the PCLOB must be consulted while intelligence agencies update their internal policies and procedures to implement the EO 14086. In addition, the PCLOB will carry out a review of the updated policies and procedures and assess their compliance with the EO 14086.¹⁸⁶ While the findings of the PCLOB are not binding *stricto sensu*, the head of each element of the Intelligence Community is obliged to carefully consider and implement or otherwise address all recommendations contained in any such review, consistent with applicable law¹⁸⁷. The EDPB invites the Commission to pay special attention to whether and how the PCLOB's recommendations have been implemented at agency level in future reviews, if the Draft Decision is adopted.
198. The EDPB recalls that the PCLOB, as it is independent, is "encouraged" to carry out but not obliged to review, if the safeguards constituted in EO 14086 are properly considered and whether the Intelligence Community fully complied with the requirements of the redress process. However, it is the

¹⁸⁴ See, e.g. Inspector General Act of 1978, § 8 (for the Department of Defence); § 8E (for the DOJ), § 8G (d)(2)(A),(B) (for the NSA); 50. U.S.C. § 403q (b) (for the CIA); Intelligence Authorization Act For Fiscal Year 2010, Sec 405(f) (for the Intelligence Community).

¹⁸⁵ WP29 Opinion 01/2016.

¹⁸⁶ EO 14086, Section 2(c)(iv) and Section 2(c)(v).

¹⁸⁷ EO 14086, Section 2(c)(v)(B).

understanding of the EDPB that the PCLOB has stated in its additional explanation to the EDPB as well as in public¹⁸⁸ that it will take on the role foreseen in EO 14086.

199. Furthermore, the EDPB welcomes that the results of the PCLOBs reports are intended to be released to the public. Taking into account that the various bodies within the redress mechanism and the ones of the Intelligence Community have in principle to implement the recommendations in the reports of the PCLOB or otherwise address them, the EDPB recognises that these recommendations play an important role of privacy safeguards.
200. The EDPB notes that the PCLOB's access to information is restricted, if the U.S. President authorizes the conduct of "covert actions"¹⁸⁹ by departments, agencies or entities of the United States Government.¹⁹⁰
201. Following its previous opinions, the EDPB considers the PCLOB as an independent body, whose recommendations have been an important contribution to reforms in the U.S. and whose reports have been a particularly helpful source to understand the functioning of the various surveillance programs, to be an essential element of the oversight structure.
202. However, the EDPB regretted in its 3rd Annual Joint Review of the former EU-U.S. Privacy Shield that the PCLOB provided the EDPB only with the same information as the general public. Furthermore, it was regrettable that the PCLOB did not issue further reports on PPD-28 to follow up on its first report in order to provide additional elements as to how the safeguards of PPD-28 are applied, as well as a general updated report on Section 702 FISA.
203. Therefore, the EDPB welcomes the announcement of the PCLOB towards the EDPB, that the publication of a follow up report on Section 702 FISA can be expected in the near future. Furthermore, the EDPB is satisfied that the PCLOB informed about its commitment to allow publicity of its reports regarding the EO 14086. However, the EDPB recalls that the release of unclassified reports is regulated by U.S. law and must be coordinated with the Agencies of the Intelligence Community and cannot be decided by the PCLOB on its own accord.
204. Therefore, if the Draft Decision is adopted, the EDPB recalls that in future reviews of the EU-US data protection framework, the EDPB security cleared experts should be able to review additional documents and discuss additional classified elements as necessary to ensure that the information in the reports can be adequately assessed, while taking into account relevant national security interests and applicable privacy protections.
205. The EDPB welcomes the PCLOB's independence and oversight of the national intelligence community, which has to comply with the recommendations of the PCLOB or otherwise address it, which will be indicated in the report of the PCLOB to the U.S. Congress.

¹⁸⁸ [https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20\(FINAL\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf)

¹⁸⁹ According to 50 U.S.C. §3093(e)(1) the term "covert action" means an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly, but does not include (1) activities the primary purpose of which is to acquire intelligence, traditional counterintelligence activities [...].

¹⁹⁰ 42 U.S.C. § 2000ee (g) (5); 50 U.S. Code § 3093(a)

206. Taking into account the requirements of the ECtHR regarding public scrutiny¹⁹¹ that the reports of a supervisory body have to be laid before and discussed by Parliament, the EDPB considers it sufficient, that the PCLOB submits its reports not less than semiannually to the U.S. President and in particular to the Congressional committees of the Senate and House of Representatives¹⁹², which are the parliamentarian bodies of the U.S.

3.2.3.3.2 Foreign Intelligence Surveillance Court (FISC)

207. The Foreign Intelligence Surveillance Court is responsible for the oversight of the collection of personal data pursuant to Section 702 FISA¹⁹³ and the decisions of the FISC can be appealed to the Foreign Intelligence Surveillance Court of Review (FISCR).
208. The FISC oversees the certification process for the collection of foreign intelligence information pursuant to Section 702 FISA and authorizes electronic surveillance, physical search and other investigative measures for foreign intelligence purposes.¹⁹⁴ The FISC also authorizes the procedures for targeting, minimizing and querying the certificates, which are legally binding on U.S. intelligence agencies.¹⁹⁵ If the FISC finds that the requirements have not been met, it may deny the certification in full or in part and require the procedures to be amended.
209. If violations of targeting procedures are identified, the FISC can order the relevant intelligence agency to take remedial action.¹⁹⁶ These remedies range from individual to structural measures, e.g. from terminating data acquisition and deleting of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training for staff.
210. The EDPB acknowledges that EO 14086 provides that the CLPO and the DPRC are to report violations to the Assistant Attorney General for National Security, who shall report those violations to the FISC¹⁹⁷.
211. As the CJEU noted in its Schrems II decision, the FISC does not authorise individual surveillance measures; rather, it authorises surveillance programs¹⁹⁸. Therefore, the EDPB maintains its concern that the FISC does not provide effective judicial oversight on the targeting of non-U.S. persons which appears not to be resolved by the new EO 14086.
212. With regard to prior independent authorisation¹⁹⁹ of surveillance under Section 702 FISA, the EDPB regrets that, as the EDPB understands from the Draft Decision²⁰⁰ and explanations provided by the U.S. Government, the FISC does not appear to be bound by the additional safeguards of the EO 14086, when certifying the programs authorising the targeting of non-U.S. persons. In the view of the EDPB, the additional safeguards contained in this order should nevertheless be taken into account in this context. The EDPB recalls that reports of the PCLOB would be particularly useful to assess how the

¹⁹¹ ECtHR Zakharov judgment, paragraph 283, ECtHR, L. v. Norway, 9 June 1990; ECtHR, Kennedy v. the United Kingdom, 18 May 2010, paragraph 166.

¹⁹² 42 U.S.C. §2000ee, (e).

¹⁹³ 50 U.S.C. 1881 (a)

¹⁹⁴ www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

¹⁹⁵ 50 U.S.C.1881a (i)

¹⁹⁶ 50 U.S.C. § 1803 (h)

¹⁹⁷ EO 14086, Section 3 (c) (i) (D); EO 14086 Section 3 (d) (i) (F)

¹⁹⁸ CJEU Schrems II judgment, paragraph 179.

¹⁹⁹ For the collection of data in bulk under EO 12333 where the FISC is not competent, the EDPB is concerned, that there is not a prior authorization process in place for the collection of data in bulk (see also Guarantee B).

²⁰⁰ Draft Decision, recital 165.

safeguards of the EO 14086 will be implemented and how these safeguards are applied when data is collected under Section 702 FISA.

3.2.4 Guarantee D - Effective remedies need to be available to the individual

213. The EDPB recalls that effective and enforceable rights of the individual are of fundamental importance for the finding of an adequate level of data protection in a third country. Data subjects must have an effective remedy to satisfy their rights when they consider that they are not or have not been respected. The CJEU explained in its Schrems I and II decisions that “legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.”²⁰¹
214. The U.S. system relating to judicial remedies contains an important limit that makes it very difficult to bring legal proceedings against surveillance measures by the U.S. Government before ordinary courts. The U.S. constitution requires an individual to demonstrate standing, i.e. to establish a “concrete, particularized, and actual or imminent injury”.²⁰² In surveillance cases such requirement appears to be nullified by the lack of notification to individuals subjected to surveillance even after these measures have ended.
215. In this context, the EDPB welcomes that EO 14086 establishes a specific redress mechanism to handle and resolve complaints from non-U.S. individuals, concerning U.S. signals intelligence activities. Under this new mechanism, the standing requirement is not applicable: according to Section 4(k)(ii) of EO 14086, the claimant does not need to show that their data has in fact been subject to U.S. signals intelligence. Data subjects can thus invoke the safeguards provided for in EO 14086, including those foreseen by other relevant laws and provisions as referred to in Section 4(d)(iii) of EO 14086.²⁰³ In this regard, the new mechanism adds a redress avenue which would otherwise not exist.
216. The new mechanism comprises two layers: Under the first layer, individuals are able to lodge a complaint with the Civil Liberties Protection Officer of the Office of the Director of National Intelligence (CLPO). At the second level, individuals have the possibility to appeal the decision of the CLPO before a newly created body, the so-called Data Protection Review Court (DPRC). The following sections primarily focus on the second tier of the redress mechanism. The EDPB considers that the CLPO, as acting government official, is not vested with a sufficient degree of independence from the executive and thus cannot, of itself, adequately fulfill the requirements following from Article 47 of the Charter. This assessment has been confirmed by the Commission on several occasions.

3.2.4.1 *Can the establishment of the DPRC based on an Executive Order per se be sufficient*

217. The DPRC is not an ordinary court established by Congress under Article III of the U.S. constitution but is based on an Executive Order issued by the U.S. President. While the EDPB is aware of and generally welcomes the underlying consideration, namely avoiding the requirement to demonstrate standing (see also paragraph 215), this raises a fundamental question: Can such redress mechanism meet the requirements of Article 47 of the Charter (at all)? According to this provision everyone whose rights

²⁰¹ CJEU Schrems I judgment, paragraph 95; CJEU Schrems II judgment, paragraph 187.

²⁰² Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. p.10.

²⁰³ EO 14086, Section 5(h) explicitly creates an entitlement for data subjects to submit complaints in accordance with the redress mechanism.

and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal previously established by law.

218. While the English wording of Article 47 of the Charter refers to a “tribunal”, other language versions give preference to the word “court”.²⁰⁴ In Schrems II the CJEU has reiterated that “data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data”.²⁰⁵ However, in the same context of assessing the adequacy of the level of data protection, the CJEU considers that an effective judicial protection against such interferences can be ensured not only by a court, but also by a body, which offers guarantees essentially equivalent to those required by Article 47 of the Charter.²⁰⁶ Likewise, the ECHR stipulates that “everyone whose rights and freedoms are violated shall have an effective remedy before a national authority”²⁰⁷, which, as the ECtHR has consistently held, does not necessarily have to be a judicial authority.²⁰⁸ Rather, the powers and procedural guarantees an authority possesses, in particular whether it is independent of the executive and ensures the fairness of the proceedings, are relevant to assessing the effectiveness of the remedy before that authority.²⁰⁹ It appears that both courts do not base their assessment on purely formalistic criteria, but regard the substantive safeguards as decisive.
219. In Schrems II the CJEU has paid particular attention to effective redress in the area of national security access to personal data. The EDPR takes note that in doing so, the CJEU however did not discuss the “previously established by law” element of Article 47 of the Charter even though the Privacy Shield Ombudsperson mechanism was as well not based on U.S. statutory law. Instead of addressing this issue, the CJEU assessed different aspects for its adequacy test, such as the lack of remedial powers. Thus, the Schrems II judgment does not provide any guidance on the assessment of “previously established by law” according to Article 47 of the Charter. However, there are other rulings in which the CJEU has commented on this matter. Echoing the settled case-law of the ECtHR in that regard, the CJEU recalled in its cases C-487/19 and C-132/20 that the reason for the introduction of the term “previously established by law” is to ensure that the organisation of the judicial system in a democratic society does not depend on the discretion of the executive, but that it is regulated by law emanating from the legislature in compliance with the rules governing its jurisdiction.²¹⁰ As can be seen from this statement, the right to a tribunal previously established by law is very closely related to the guarantee of independence.
220. Against this background, the EDPR concludes that, in the context of assessing the adequacy of the level of protection, the specific redress mechanism created under EO 14086 as opposed to redress in Article III courts is not per se insufficient. The analysis of the level of protection in this respect depends on whether the safeguards provided in EO 14086 and complemented by the AG Regulation sufficiently ensure the independence of the DPPC vis-à-vis the other powers.
221. The Commission should continuously monitor whether the rules set forth in EO 14086 and its supplemental provisions, in particular those designed to foster the DPPC's independence, are fully

²⁰⁴ For example “Gericht” in the German language version.

²⁰⁵ CJEU Schrems II judgment, paragraph 194.

²⁰⁶ See CJEU Schrems II judgment, paragraph 197.

²⁰⁷ Article 13 ECHR.

²⁰⁸ ECtHR Klass judgment, paragraph 67; ECtHR Big Brother Watch judgment, paragraph 359.

²⁰⁹ ECtHR Klass judgment, paragraph 67; ECtHR Big Brother Watch judgment, paragraph 359.

²¹⁰ See CJEU, C-487/19, judgment of 6 October 2021, W.Z., ECLI:EU:C:2021:798 and C-132/20, judgment of 29 March 2022, Getin Noble Bank S.A., ECLI:EU:C:2022:235, paragraph 129 and paragraph 121.

implemented and are functioning effectively in practice. In addition, any amendments of the framework should be carefully reviewed for the impact on the Commissions assessment according to the Draft Decision. In this regard, the EDPB notes that changes to EO 14086 and the AG Regulation may trigger the adoption of immediately applicable implementing acts suspending, repealing or amending the adequacy decision.²¹¹

3.2.4.2 Sufficient independence from the executive

222. In its Schrems II ruling, the CJEU underlined that the independence of the court or body has to be ensured, especially from the executive, with all necessary guarantees, including with regard to its conditions of dismissal or revocation of the appointment. More specifically, the CJEU has criticized the fact that the Ombudsperson was appointed by and directly reporting to the Secretary of State. The Ombudsperson was held to be an integral part of the U.S. State Department. The CJEU also found there were no particular guarantees for the dismissal or revocation of the appointment of the Ombudsperson, hence undermining the Ombudsperson's independence from the executive.
223. The EDPB acknowledges that the provisions of EO 14086 and the supplemental AG Regulation do not impose a reporting obligation on the DPRC to the Attorney General, as would be the case in a superior-subordinate relationship. Nor is the DPRC subject to the Attorney General's "day-to-day supervision"²¹². These safeguards are a significant improvement over the Privacy Shield. However, the DPRC is established within the executive branch, namely the Department of Justice. For this reason in particular, the implementation and effective functioning of the safeguards in practice will be critical to determining whether the DPRC, although not an integral part of the Department of Justice, as an entity nevertheless located within the executive, can be considered sufficiently independent in practice. The EDPB calls on the Commission to monitor carefully whether these safeguards are fully reflected in practice. In addition, the EDPB suggests to clarify the term "day-to-day supervision" to the end that the "judges" of the DPRC are not subject to supervision of any kind. The Commission has confirmed that "day-to-day supervision" is meant to be understood in this sense.
224. Further to the above safeguards, the EU-U.S. DPF foresees certain guarantees regarding the appointment and dismissal of the DPRC "judges". While they are appointed by the Attorney General, their appointment is based on the criteria used to evaluate applicants for federal judgeships and involves a consultation of the PCLOB. Dismissal of "judges" prior to the expiration of their term of office or from an ongoing proceeding is possible only in narrowly defined circumstances, which, as the EDPB understands, are modeled on the provisions applicable to federal judges.²¹³ The application of these rules represents a further step to strengthen the independent position of the DPRC for which, again, implementation in practice will be crucial. However, it is not clear from the Draft Decision as such whether and how compliance with these requirements will be observed in the United States. Based on additional explanations provided by the Commission and the U.S. Government, the EDPB understands that the PCLOB may address the above mentioned provisions in its annual review of the redress process and that the responsibility to monitor and ensure compliance with all legal requirements of the Inspector General within the Department of Justice includes the requirements in EO 14086 and the regulations establishing the DPRC. The EDPB invites the Commission to clarify this aspect in the Draft Decision. That being said, the Commission should take these safeguards into account when monitoring the actual practice of the processing of personal data as assessed in the Draft Decision.

²¹¹ Draft Decision, recital 212.

²¹² AG Regulation, § 201.7 (d).

²¹³ EO 14086, Section 3(d)(iv); AG Regulation § 201.7.

225. The Draft Decision does not address the question whether, and if so, under which conditions the U.S. President has the authority to dismiss or remove “judges” from the DPRC. It is the understanding of the EDPB that such authority would not exist, as has been explained by the European Commission and confirmed by representatives of the U.S. government. The EDPB suggests to clarify this aspect in the adequacy decision.
226. The “judges” of the DPRC are appointed for four-year renewable terms and, at the time of their initial appointment, must not have been employed in the executive branch in the previous two years.²¹⁴ During their term of appointment as “judges” on the DPRC, they shall not have any other official duties or employment within the U.S. government.²¹⁵ They may however, unlike U.S. federal judges, participate in extrajudicial activities, including business activities, financial activities, non-profit fundraising activities, fiduciary activities, and the practice of law, where such activities do not interfere with the impartial performance of their duties or the effectiveness or independence of the DPRC.²¹⁶ Judicial independence derives not only from the freedom from instructions, but also from personal independence. In this context, factors such as the term of office, the possibility to be reappointed and the potential for conflicts of interest are relevant. The term of four years foreseen under EO 14086 and respectively the AG Regulation, while being e.g. shorter than the terms of office of judges of the CJEU (six years with the possibility of reappointment) and ECtHR (nine years without the possibility of reappointment), but as such does not give rise to serious concerns. The EDPB is not aware of any case-law imposing a minimum term of office in this respect²¹⁷. The EDPB also recognises that the possibility to engage in extrajudicial activities is subject to the condition that, simply put, they do not lead to conflicts of interest compromising the duties on the DPRC. The EDPB understands from the U.S. Government’s additional explanations that these requirements are as well subject to the review and monitoring by the PCLOB and the Inspector General of the Department of Justice (see supra paragraph 226). How this requirement will be applied and demonstrated in practice should as well be addressed as part of the joint reviews.
227. Pursuant to Section 3(d)(i)(B) EO 14086 all “judges” of the DPRC must hold security clearances to be able to access classified information, i.e. to carry out their very function of adjudicating national security cases.²¹⁸ Some European laws and regulations on security clearance, in contrast, exempt judges from the requirement of a security clearance to the extent they perform judicial duties, regarding such detailed scrutiny as potentially conflicting with judicial independence.²¹⁹ According to explanations by the U.S. Government, while a candidate for a judicial appointment in a U.S. court undergoes a thorough vetting, after being appointed to serve as a federal judge in a U.S. court, a federal judge is not required to obtain a security clearance to access classified documents relevant to the case.
228. In the EDPB’s view, the circumstances outlined above partly reveal differences between the position and status of a U.S. federal judge and a “judge” on the DPRC. However, the safeguards provided do not give reason to doubt the DPRC’s independence. The EDPB urges the Commission that, should the Draft Decision be adopted, the above-mentioned safeguards be a priority during the first joint review

²¹⁴ AG Regulation § 201.3 (a).

²¹⁵ AG Regulation § 201.3 (c).

²¹⁶ AG Regulation § 201.7 (c).

²¹⁷ See also, mutatis mutandis, ECtHR (Grand Chamber), Case of Centrum För Rättvisa V. Sweden, 25 May 2021, paragraph 346.

²¹⁸ See also AG Regulation § 201.11 (b) and Draft Decision, recital 177.

²¹⁹ E.g. § 2(3) German Security Clearance Law.

of the EU-U.S. DPF. Furthermore, the EDPB expects the Commission to follow up on their commitment to suspend, repeal or amend the decision, if adopted, in case the U.S. Executive chooses to restrict the safeguards included in the EO²²⁰.

3.2.4.3 Powers of the DPRC

3.2.4.3.1 Access to information

229. Effective legal protection requires that a court has sufficient investigatory powers to review the contested measure. In the Kadi II case the CJEU ruled in regard to Article 47 of the Charter that the Courts of the European Union are to ensure that a decision is taken on a sufficiently solid factual basis.²²¹ The CJEU states that “it is for the Courts of the European Union, in order to carry out that examination, to request the competent European Union authority, when necessary, to produce information or evidence, confidential or not, relevant to such an examination”²²², whereby “the secrecy or confidentiality of [...] information or evidence is no valid objection”²²³.
230. Pursuant to Recital 181 of the Draft Decision the DPRC reviews the determinations made by the CLPO based, at a minimum, on the record of the CLPO’s investigation, as well as any information and submissions provided by the complainant, the Special Advocate or an intelligence agency. The Draft Decision further states that the DPRC has access to all information necessary, which it may obtain through the CLPO. This is based on the provision of § 201.9(b) AG Regulation, which authorizes the DPRC to “request that the ODNI CLPO supplement the record with specific explanatory or clarifying information and that the ODNI CLPO make additional factual findings where necessary to enable the DPRC panel to conduct its review”. It is the understanding of the EDPB that the assessment carried out by the DPRC is thus not in any way limited to the findings made by the CLPO at the first level of the new redress mechanism. On the contrary, the DPRC can seek both additional legal information and, importantly, further factual circumstances for its analysis of whether a covered violation has occurred. At the same time, the EDPB also notes that these generally extensive investigatory powers do not extend to direct access to the data held on the individual. The Commission has explained that the CLPO will always function as an intermediary when the DPRC requires further information. Therefore, the DPRC’s access to information necessary to independently adjudicate an application for review relies, to a certain extent, on the CLPO providing the necessary information. The EDPB recognises that the CLPO has an obligation to “provide any necessary support” to the DPRC and intelligence agencies are obliged to provide the CLPO with access to information necessary to conduct the DPRC’s review²²⁴. The EDPB also notes, however, that the CLPO itself is not independent and conducts the initial investigation of a complaint at the first stage of the redress procedure. Therefore, the EDPB welcomes that the PCLOB will verify during its annual reviews of the redress mechanism whether the DPRC has obtained full access to all necessary information²²⁵. In addition, the EDPB invites the Commission to include this aspect in the joint reviews, if the Draft Decision is adopted, to examine the implications of this system in practice.

²²⁰ Draft Decision, recital 212.

²²¹ CJEU, Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, European Commission and Others v Yassin Abdullah Kadi, judgment of 18 July 2013 (hereinafter, ‘CJEU Kadi II judgment’), paragraph 119.

²²² CJEU Kadi II judgment, paragraph 120.

²²³ CJEU Kadi II judgment, paragraph 125.

²²⁴ EO 14086, Section 3(c)(i)(H) and Section 3(d)(iii).

²²⁵ EO 14086, Section 3(e)(i).

3.2.4.3.2 Remedial powers

231. One of the central deficiencies of the Privacy Shield that led to its invalidation by the CJEU in Schrems II was the lack of binding remedial powers for the Ombudsperson. The CJEU found that “there is nothing [...] to indicate that that ombudsperson has the power to adopt decisions that are binding on those intelligence services”.²²⁶ The mere (political) commitment from the U.S. Government that the Intelligence Community would correct any violation of the applicable rules detected by the Ombudsperson did not suffice to ensure a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter.
232. Under the new redress mechanism, by contrast, the decisions taken by the CLPO and by the DPR have binding effect.²²⁷ The EDPB recognizes, on the one hand, that this authority is not limited to specific measures, but allows “appropriate remediation” to “fully redress” an identified covered violation. Notably, Section 4(a) of EO 14086 explicitly mentions the deletion of unlawfully collected data. On the other hand, the EDPB notes that the wording of Section 4(a) of EU 14086 creates some uncertainty as to the process of determining such “appropriate remediation”. While a measure should be designed to fully redress a violation, consideration should also be given to “the ways that a violation of the kind identified have customarily been addressed”.²²⁸ The meaning and effect of such requirement is unclear. Therefore, the EDPB invites the Commission to closely monitor the remediation measures adopted in practice.

3.2.4.4 Filing a complaint under the new redress mechanism

233. The redress mechanism established under EO 14086 is only applicable to qualifying complaints transmitted by the appropriate public authority in a qualifying state concerning United States signals intelligence activities for any covered violation.²²⁹ Hence, in order to avail oneself of this legal protection, several conditions need to be fulfilled.

3.2.4.4.1 Designation as qualifying state

234. First of all, the country or regional economic integration organization, from where the data was transferred to the United States must have been designated as a qualifying state prior to the data transfer underlying the complaint.²³⁰ It is evidently essential that the redress mechanism provided is available when the adequacy decision enters into application. Accordingly, Recital 196 of the Draft Decision provides that the entry into force of the decision is conditional, *inter alia*, on the designation of the Union as a qualified entity for the purposes of the redress mechanism. In fact, the Commission appears to assume that the designation will occur prior to the adoption of the decision, as the draft already includes a placeholder for the Attorney General’s designation of the EU²³¹ (as opposed to including the designation as a condition precedent in the operative part of the Draft Decision).

3.2.4.4.2 Adverse affect on privacy and civil liberties interests and “standing”

235. A “qualifying complaint” needs to be based on an alleged “covered violation”, which in turn requires a violation that adversely affects the complainant’s individual privacy and civil liberties interests²³². It is

²²⁶ CJEU Schrems II judgment, paragraph 196.

²²⁷ EO 14086, Section 3(c)(ii) and Section 3(d)(ii), respectively.

²²⁸ EO 14086, Section 4(a).

²²⁹ EO 14086, Section 3(a).

²³⁰ EO 14086, Sections 4(d)(i), 4(k)(i).

²³¹ Draft Decision, footnote 320.

²³² EO 14086, Section 4(k)(i) and 4(d)(ii).

the understanding of the EDPB, based on additional explanations from the Commission, that “adversely affect” does not imply any form of restriction on the admissibility of a complaint. Rather, as the Commission stated, such adverse affect would pertain to any complaint concerning the processing of personal data for signals intelligence activities in violation of the provisions referred to in Section 4(d)(iii), e.g. the safeguards of EO 14086. The EDPB regrets that this is not specified in the text of the Draft Decision and invites the Commission to further clarify the notion of being “adversely affected” in order to ensure that any violation of the data subjects’ rights are assessed and remediated and that there is no level of “gravity” to be demonstrated to have access to redress and appropriate remediation.

236. As already mentioned, a complaint under EO 14086 does not require the claimant to demonstrate standing (see paragraph 215)²³³. The EDPB welcomes the clarification in Section 4(k) EO 14086 that a “belief test” will be applied and that it is not necessary to show that the complainant’s data has in fact been accessed through signal intelligence activities. The establishment of the redress mechanism is an important step, as the standing requirement makes it very difficult to challenge surveillance measures before ordinary courts in the United States.
237. Based on the above, the EDPB does not consider recourse to ordinary courts, to which the Draft Decision also refers²³⁴, to offer an adequate level of protection²³⁵. In this regard, the EDPB recalls its concerns already many times expressed in relation to the standing requirement before ordinary courts²³⁶. Moreover, based on additional statements by the U.S. government, it is the understanding of the EDPB that while EO 14086 does not preclude recourse to the courts of general jurisdiction, it is uncertain how such a court would apply this Order. This question could be explored further in the future reviews, if the Draft Decision is adopted.

3.2.4.4.3 The procedure of a complaint

238. The EDPB endorses in principle the procedure for routing a complaint through supervisory authorities of the Member States and continues to believe that the identification of the complainant should take place on EU territory. However, as under the Privacy Shield Ombudsperson mechanism, the Draft Decision provides that a data subject who wishes to lodge such a complaint must submit it to a supervisory authority in an EU Member State competent for the oversight of national security services and/or the processing of personal data by public authorities²³⁷. In this respect, the EDPB recalls its concerns already expressed in the WP 29’s Opinion on the Privacy Shield, for instance potential difficulties for individuals to identify the competent authority given the variety of supervision mechanisms of national security services in Member States²³⁸. Taking into account the involvement of the national data protection authorities in the application of and oversight on the EU-U.S. DPF it is more appropriate to channel complaints through them.

3.2.4.5 The decision of the DPRC

239. After the review of the complainant’s application is completed, the DPRC must not reveal whether or not the complainant was subject to U.S. signals intelligence activities. Instead, the complainant is

²³³ Clapper v. Amnesty International USA, 568 U.S. 398 (2013) II. p.10.

²³⁴ Draft Decision, recital 187 et seq.

²³⁵ See also CJEU Schrems II judgment, paragraphs 191, 192.

²³⁶ See WP29 Opinion 01/2016, p. 43.

²³⁷ Draft Decision, recital 169.

²³⁸ WP29 Opinion 01/2016, p. 48, 49.

notified that “the review either did not identify any covered violations or the Data Protection Review Court issued a determination requiring appropriate remediation”²³⁹. This standard response serves the generally legitimate purpose of protecting sensitive information about U.S. intelligence activities. However, the EDPB is concerned that EO 14086 does not provide for any exemptions to the standard response of the DPRC.

240. In the Kadi II case, the CJEU had to address the conflicting interests of state secrecy on the one hand and fair, and as far as possible, adversarial proceedings on the other. The CJEU ruled that in circumstances where overriding considerations to do with national security preclude the disclosure of information or evidence to the person concerned, it is none the less the task of the courts to apply, in the course of judicial review, techniques which accommodate legitimate security considerations about the nature and sources of information and the need to sufficiently guarantee the respect for the individual’s procedural rights, such as the right to be heard and the requirement for an adversarial process²⁴⁰. The CJEU further specified that it is for the courts, when carrying out an examination of all the matters of fact or law produced by the competent European Union authority, to determine whether the reasons relied on by that authority as grounds to preclude that disclosure are well founded²⁴¹. If it turns out that the reasons relied on by the competent European Union authority do indeed preclude the disclosure to the person concerned of information or evidence, it is still necessary to strike an appropriate balance between the requirements attached to the right to effective judicial protection, and those flowing from national security²⁴². In order to strike such a balance, it is legitimate to consider possibilities such as the disclosure of a summary outlining the information’s content or that of the evidence in question²⁴³. Although the court’s findings do not impose requirements for the decision issued by a court but rather relates to the decision of the competent authority and to the conduct of judicial proceedings, they provide indications about the balancing of the above mentioned interests in the context of the right to effective legal protection. For further guidance, reference can also be made to the Big Brother Watch case, in which the ECtHR, alluding to the fairness of the proceedings and in particular to the principle of an adversarial process, held that the decisions of a judicial or otherwise independent body should be reasoned²⁴⁴.
241. The EDPB recognizes that the decisions of the DPRC are indeed reasoned. The DPRC is expressly required to issue a written decision setting out its determinations and the specification of any appropriate remediation²⁴⁵. In addition, the EDPB notes that the individual will be notified if the information pertaining to a review by the DPRC has been declassified²⁴⁶. The EDPB also recognises the role of the special advocates foreseen in the new redress mechanism that includes advocating regarding the complainant’s interest in the matter²⁴⁷. However, in light of the implications of the jurisprudence of the CJEU and ECtHR set out above and taking into account that the decision of the DPRC cannot be appealed but is final²⁴⁸, the EDPB has concerns about the general application of the standard response of the DPRC. The EDPB recalls that the PCLOB will independently review the functioning of the new redress mechanism and invites the Commission to pay particular attention to

²³⁹ EO 14086, Section 3(d)(i)(H). Section EO 14086 stipulates this response for the CLPO as well.

²⁴⁰ CJEU Kadi II judgment, paragraph 125.

²⁴¹ CJEU Kadi II judgment, paragraph 126.

²⁴² CJEU Kadi II judgment, paragraph 128.

²⁴³ CJEU Kadi II judgment, paragraph 129.

²⁴⁴ ECtHR Big Brother Watch judgment, paragraph 359.

²⁴⁵ AG Regulation, § 201.9 (g).

²⁴⁶ EO 14086, Section 3(d)(v).

²⁴⁷ AG Regulation, § 201.8 (g).

²⁴⁸ AG Regulation, § 201.9 (g).

this issue, including any assessment on this aspect by the PCLOB, during future reviews of the decision, if adopted.

4 IMPLEMENTATION AND MONITORING OF THE DRAFT DECISION

242. Concerning the monitoring and review of the Draft Decision, the EDPB notes that according to the case law of the CJEU, ‘in the light of the fact that the level of protection ensured by a third country is liable to change, it is incumbent upon the Commission, after it has adopted an adequacy decision pursuant to [Article 45 GDPR], to check periodically whether the finding relating to the adequacy of the level of protection ensured by the third country in question is still factually and legally justified. Such a check is required, in any event, when evidence gives rise to a doubt in that regard’²⁴⁹.
243. In addition, the EDPB notes that the letter from the DoC provides that the DoC and other US agencies, as appropriate, will hold meetings on a periodic basis with the Commission, interested EU DPAs, and appropriate representatives from the EDPB²⁵⁰.
244. The EDPB considers that the state law protection in relation to access by law enforcement authorities, the derogation for temporary bulk collection in view of targeted collection by US national security authorities, the application in practice of the newly introduced principles of necessity and proportionality, including in the context of the UPSTREAM program, the interplay between the EO 14086 and the different U.S. legal instruments allowing U.S. intelligence agencies to collect and further process personal data, the implementing internal policies and procedures, how these safeguards will also be taken into account in the context of the oversight led by the FISC, and how the redress mechanism will function effectively, and the question of onward transfers, automated-decisions, substantive and effective oversight and enforcement of the DPF Principles as well as effective redress will deserve specific attention in the course of the next periodic reviews.
245. The EDPB notes that the review of the adequacy finding will take place after one year from the date of the notification of the adequacy decision to the Member States and subsequently at least every four years²⁵¹. With a view to further strengthening the continuous monitoring of the adequacy decision, the EDPB calls on the Commission to carry out the subsequent reviews at least every three years.
246. Concerning the practical involvement of the EDPB and its representatives in the preparation and proceeding of the future periodic reviews, the EDPB reiterates that any relevant documentation should be shared in writing with the EDPB, including correspondence, sufficiently in advance of the reviews. As was the case for the reviews carried out under the Privacy Shield, the EDPB recommends that, at the latest three months before the review should take place, the modalities for the review are established and agreed between the Commission, the US administration and the EDPB.
247. Furthermore, the EDPB notes and welcomes that Recital 212 of the Draft Decision provides examples of modifications undermining the level of protection that may justify the initiation of an ‘emergency repeal procedure’ that focuses on modifications that could occur concerning the Executive Order 14086 and the related AG Regulation.

²⁴⁹ CJEU Schrems I judgment, paragraph 76. See also Draft Decision, Article 3(4).

²⁵⁰ Draft Decision, Annex III.

²⁵¹ Draft Decision, Article 3(4).

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 2/2025 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Alfa Laval Group

Adopted on 13 March 2025

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023 (hereinafter “the Recommendations”),

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023, which supersede the working documents WP256 rev.01 and WP264 of the Article 29 Working Party².

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the Recommendations. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data³.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC. The following documents, which were endorsed by the EDPB, are now superseded by the EDPB Recommendations: Article 29 Working Party’s Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules (WP 256 rev.01) and Article 29 Working Party’s Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfers of Personal Data (WP 264).

³ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁴, applicable to the EDPB pursuant to Article 76 (2) GDPR.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Alfa Laval Holding AB and its entities (hereinafter the "**Alfa Laval Group**") was reviewed by the SE SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Alfa Laval Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 6 February 2025. The decision on the completeness of the file was taken on 20 February 2025.

2 ASSESSMENT

3. The draft BCR-C of the Alfa Laval Group covers all transfers of personal data between Alfa Laval Group entities bound by the BCR⁵.
4. Concerned data subjects include employees and their family members, job applicants, contractors, customers, suppliers and visitors to the Alfa Laval Group's premises and webpages⁶.
5. The draft BCR-C of the Alfa Laval Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Alfa Laval Group contains all the elements required under Article 47 GDPR and the Recommendations, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement⁷, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Alfa Laval Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ BCR-C, section 3.2.

⁶ BCR-C, section 3.2 and Annex 4.

⁷ Alfa Laval Intra-Group BCR Agreement.

be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and the Recommendations providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 8/2019 on the competence of a supervisory authority in case of a change in circumstances relating to the main or single establishment

Adopted on 9 July 2019

Table of contents

1	SUMMARY OF THE FACTS.....	3
2	ON THE COMPETENCE OF THE BOARD TO ADOPT AN OPINION UNDER ARTICLE 64.2 ON THIS TOPIC	4
3	RELEVANT PROVISIONS	5
4	OPINION OF THE EDPB	6
4.1	Scope of the opinion	6
4.2	The rationale for the opinion	6
4.3	The adopted opinion	8
4.3.1	Relocation of the main or single establishment within the EEA	8
4.3.2	Creation of the main or single establishment or relocation from a third country to the EEA	8
4.3.3	Disappearance of the main or single establishment.....	9
5	CONCLUSION	10

The European Data Protection Board

Having regard to Article 63 and Article 64(2) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the “Board”) is to ensure the consistent application of the GDPR throughout the European Economic Area. Article 64(2) of the GDPR provides that any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one EEA Member State be examined by the Board with a view to obtaining an opinion. The aim of this opinion is to examine a matter of general application or which produces effects in more than one EEA Member State.

(2) On April 30, 2019, the French and the Swedish Data Protection Authorities requested the Board to examine and issue an opinion on continuance of the competence of a national authority in case of a change in circumstances relating to the main or single establishment.

(3) The opinion of the Board shall be adopted pursuant to Article 64(3) of the GDPR in conjunction with Article 10(2) of the Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authorities have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The French and the Swedish data protection authorities requested the Board to examine and issue an opinion on continuance of the competence of a national authority in case of a change in circumstances relating to the main or single establishment.
2. These changes may occur when:
 - a single or main establishment is relocated from one EEA country to another EEA country;
 - a single or main establishment ceases to exist on the EEA territory;

- a main establishment is set up on an EEA country's territory or moves from a third country to an EEA country.
3. The French and the Swedish data protection authorities specifically submitted the following questions :
- As of when should an authority's competence be considered as definitely fixed, rendering any change relating to the main or single establishment's circumstances without effect on the procedure?
 - Should this be the initial moment when a complaint is received by an authority or, if not based on a complaint, when the authority starts looking at a processing at its own discretion?
 - Should this be the moment when an authority decides to initiate an investigation and contacts the controller/processor?
 - Should it be the moment when a decision-making procedure is launched?
 - Should this be the moment when the authority renders a decision thereby putting an end to the case in question?
4. The decision on the completeness of the file was taken on 17 May 2019. The period until which the opinion has to be adopted has been set until 12 July.

2 ON THE COMPETENCE OF THE BOARD TO ADOPT AN OPINION UNDER ARTICLE 64.2 ON THIS TOPIC

5. The Board considers that the question of competence of a national authority in case of a change in circumstances relating to the main or single establishment concerns a "*matter of general application*" of the GDPR, as there is a clear need for a consistent interpretation among data protection authorities on the boundaries of their competences. Clarification is particularly needed to ensure, amongst others, a consistent practice of cooperation in accordance with Article 60, mutual assistance in accordance with Article 61 of the GDPR and joint operations in accordance with Article 62 of the GDPR.
6. Indeed, the GDPR does not contain any specific provision relating to the case in which the main or single establishment of the controller or processor is set up on the territory of one EEA Member State and relocated mid-procedure to another Member State's territory or outside the European Economic Area, nor to the case in which an establishment is created inside the European Economic Area mid-procedure or ceases to exist.
7. Likewise, to date, EDPB guidelines, and particularly those relating to the lead supervisory authority, do not provide any more information than the GDPR does as regards these situations.
8. Yet, to enable consistent implementation across the European Economic Area, an objective criterion must be found to fix the moment from which any change in circumstances would have no effect on the competence acquired by an authority. This issue is of significant importance as the matter of the potential concurrent competences between supervisory authorities need to be addressed. It is thus necessary, not only from the perspective of legal certainty, but also from an operational perspective (case handling by data protection authorities), to clarify the questions raised.

9. For these reasons the Board considers that the questions raised by the French and the Swedish data protection authorities can be subject to an opinion under Article 64.2.

3 RELEVANT PROVISIONS

10. Article 4.3 of the Treaty on European Union provides: "*Pursuant to the principle of sincere cooperation, the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. The Member States shall take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union. The Member States shall facilitate the achievement of the Union's tasks and refrain from any measure which could jeopardise the attainment of the Union's objectives.*"
11. Article 41(1) of the EU Charter of Fundamental Rights provides that: "*Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union*".
12. Article 51(1) of the GDPR sets forth the legal mandate of data protection authorities, which is to monitor the application of the GDPR in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the European Economic Area.
13. Articles 55, 57 and 58 specify the competence, tasks and powers of each data protection authority¹.
14. Article 56 provides for the "*one-stop shop*" mechanism, a procedural rule according to which a specific role is granted to a lead supervisory authority, defined as the authority on the territory of which the controller or processor has its main or single establishment².
15. Chapter VII of the GDPR, entitled "*Cooperation and Consistency*", defines the different ways in which data protection authorities shall cooperate in order to contribute to a consistent application of the GDPR. The relevant provisions are set out in particular in Article 60 of the GDPR, which provides for the cooperation between the lead supervisory authority and the other supervisory authorities

¹ It should be recalled in this respect that Recital 11 of the GDPR stipulates as follows: "*Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States*". Recital 13 of the GDPR states that one of the objectives of the Regulation is "*to provide legal certainty and transparency for economic operators [...] as well as effective cooperation between the supervisory authorities of different Member States*". Lastly, pursuant to Recital 122, "*Each supervisory authority should be competent on the territory of its own Member State to exercise the powers and to perform the tasks conferred on it in accordance with this Regulation*".

² Recital 124 provides that: "*Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union and the controller or processor is established in more than one Member State, or where processing taking place in the context of the activities of a single establishment of a controller or processor in the Union substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor or for the single establishment of the controller or processor should act as lead authority*".

concerned³. Likewise, under Articles 61 and 62 of the GDPR, supervisory authorities shall provide each other with mutual assistance and, where appropriate, conduct joint operations, including joint investigations and joint enforcement measures.

4 OPINION OF THE EDPB

4.1 Scope of the opinion

16. In the context of the present opinion, the Board is of the view that the questions mainly relate to infringements of a continuing or continuous nature due to the fact that, for a change in circumstances relating to the main or single establishment to intervene, the infringements need to have been committed over a certain period of time. A “continuing” infringement is an act (or omission) which lasts over a certain period of time and a “continuous” infringement is an offence consisting of several acts all of which contain the elements of the same (or similar) offence committed over a certain period of time (*European Court of human rights, grand chamber, case of Rohlena v. the Czech Republic, application no 59552/08*).

4.2 The rationale for the opinion

17. The EDPB underlines that the rules of the GDPR on distribution of competences among the different concerned Member State authorities and the concept of lead authority are based on intense and fluent co-operation among the SAs. This new level of cooperation is deriving from the fact that the GDPR is now the common legal framework for data protection, so there should be no doubt or obstacle for SAs on the consistent and swift application of the GDPR. Therefore when considering the right answer to the question raised the efficient cooperation of SAs based on mutual trust is taken as a starting point and a must.
18. To enable consistent implementation across the European Economic Area, an objective criterion must be found to solidify the moment from which any change in circumstances would have no effect on the competence acquired by an authority. Such criterion should meet three objectives:
 - to ensure both data controller and data subjects a sufficient degree of legal certainty and foreseeability, an objective stated in the GDPR and particularly in Recital 13;
 - to take into account considerations relating to good administration, by ensuring the efficiency and effectiveness of action taken by authorities (see in particular Article 41 of the CFR EU and Recitals 11 and 13 of the GDPR) and by avoiding any misuse of the one-stop shop mechanism in the form of forum shopping or forum “hopping”;
 - to limit the risk of concurrent competences between authorities.
19. Article 55(1) and Recital 122 of the GDPR set out the general principles regarding competence of SAs, whereby each supervisory authority is competent on the territory of its own Member State “*for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with*

³ This is supported by Recitals 123 to 126 and 130. More specifically, according to recital 125, “(...) *In its capacity as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process*”. Recital 126 states that “*The decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned and should be directed towards the main or single establishment of the controller or processor (...)*”.

this Regulation". However, Article 56(1) and Recital 124 contain an overriding rule and provide that the supervisory authority of the main establishment or of the single establishment of the controller or processor is competent to act as LSA for the cross-border processing carried out by that controller or processor.

20. Article 56(1) is *lex specialis*, and as such it takes priority whenever any processing situation arises that fulfils the conditions specified therein – such as the one where there is a main or single establishment in the EU that is responsible for cross-border processing activities involved in a complaint/alleged detected or reported infringement. Accordingly, a LSA's competence for handling a case arises from the existence of the controller's/processor's main or single establishment on the territory of its MS in the context of a cross-border processing activity. If the main or single establishment moves once a proceeding has been initiated before or by the LSA, and if the new main or single establishment fulfils the conditions for being considered as such, then the controller/processor will be entitled to rely on a new sole interlocutor under Article 56.1 and 56.6, *i.e.*, the new LSA in the Member State of the new main or single establishment.
21. The switch of the role as LSA does not mean that the initial SA was not competent to act at the time it did, and therefore it does not retroactively deprive the operations already carried out by the initial authority of a legal basis. The previously competent SA had full jurisdiction when the main or single establishment was located on its territory. Therefore, the acts performed retain their value and the evidence and information gathered by former LSA can be used by the newly competent one.
22. This solution increases the chances for the deciding authority to have the power to enforce its decision. Indeed, the new LSA is in a position to enforce the decision it renders as there is an establishment of the controller or processor on its territory, which is in line with the principle of effective enforcement set out in Recital 11 of the GDPR.
23. Furthermore, this solution also offers the advantage of reducing the risk of two authorities (or more) considering themselves to be the lead for the same infringement or, on the contrary, no authority considering itself to be the lead. Indeed, the criterion of a final decision being reached is relatively straightforward and its satisfaction quite easy to determine.
24. In any event, it is worth underlying that in case of change of LSA, the cooperation procedure set forth under Article 60 will be applicable and the new LSA will be under an obligation to cooperate with the former LSA and with other CSAs in an endeavour to reach consensus, at least if the former LSA remains a CSA. In practice, this means that the new LSA will have to submit a draft decision to the former LSA (and all the other concerned SAs), which as any other CSA will be in a position to express a relevant and reasoned objection. Moreover, the former LSA will be in a position to participate in the carrying out of the investigations in the context of joint operations pursuant to Article 62 if it meets the criteria set out in Article 4(22).
25. The fact that a final decision has been reached in a cooperation procedure initiated under Article 60 GDPR must be taken into due account in particular by ensuring that the initial (L)SA is involved in any subsequent steps by the newly established LSA so as to avoid depriving the administrative process of its effectiveness and/or introducing further delays in making available the relevant remedies (also in accordance with Article 41 of the CFR EU).

26. Lastly, it shall be noted that to prevent forum shopping and ensure an effective protection of data subjects, the relocation of the main establishment needs to be effective and proven by the data controller (see the WP244 entitled "*Guidelines for identifying a controller or processor's lead supervisory authority*" adopted on 13 December 2016 by the Article 29 Data Protection Working Party, p.8). The concept of the main establishment itself indicates that it is not just a momentary or only a bureaucratic step to define it by the undertaking, but a real one, made with a lasting purpose. Therefore, SAs should exercise effective control over the notion of main establishment in order to reduce the risk that controllers or processors artificially change their main establishment for the purpose of changing the competent authority to handle the case.

4.3 The adopted opinion

4.3.1 Relocation of the main or single establishment within the EEA

27. Subject to the above considerations, the relocation of the main establishment to the territory of another EEA Member State mid-procedure is considered to deprive the first authority of its original competence at the moment such a change becomes effective, but not to retrospectively deprive the operations already carried out by the initial authority of a legal basis.
28. Every pending proceeding will be transferred to the SA of the state in which the main establishment is located. This SA will become LSA, and the proceeding will continue in accordance with the rules laid down in Article 60, in cooperation with the CSA referred to in Article 4(22).
29. The relocation of the main or single establishment within the EEA is considered to deprive the first authority of its original role as LSA at the moment such a change becomes effective and demonstrated. As previously, the cooperation procedure set forth under Article 60 will be applicable and the new LSA will be under an obligation to cooperate with the former LSA and with other CSAs in order to reach consensus.

4.3.2 Creation of the main or single establishment or relocation from a third country to the EEA

30. The EDPB considers that the lead competence can switch to another SA until a final decision is made by the LSA. As a result, the creation of a main or single establishment or its relocation from a third country to the EEA (in a procedure which was initially started without cooperation) mid-procedure will allow the controller to benefit from the one-stop-shop.
31. Every pending proceeding (necessarily non-cooperation proceeding because of the initial lack of main establishment in the EEA) will be transferred to the SA of the state in which the main establishment is located. This SA will become LSA, and the proceeding will continue in accordance with the rules laid down in Article 60, in cooperation with the CSA referred to in Article 4(22).
32. The creation of a main or single establishment or its relocation from a third country is considered to deprive the first authority of its original role as a competent authority due to the fact that the complaint has been first lodged with the SA, at the moment such a change becomes effective and demonstrated. As previously, the cooperation procedure set forth under Article 60 will be applicable

and the new LSA will be under an obligation to cooperate with the former LSA and with other CSAs in an endeavour to reach consensus.

4.3.3 Disappearance of the main or single establishment

33. The EDPB considers that the lead competence can switch to another SA until a final decision is made by the LSA. As a result, the disappearance of the main or single establishment mid-procedure (either because the main establishment has been moved out of the EEA territory or because it has been disbanded) will divest the controller to benefit from the one-stop-shop.
34. In the case in which the establishment ceases to exist in the territory of its Member State, the former lead supervisory authority remains competent like any other CSA under Article 4(22) of the GDPR. Since the processing cannot be considered as cross border any more, the principle of cooperation vanishes and each concerned authority regains full jurisdiction.

5 CONCLUSION

35. In conclusion, the Board considers that competence to act as lead supervisory authority can switch to another supervisory authority in case of a documented change in the circumstances relating to the main or single establishment of a controller or processor until a final decision has been reached by that supervisory authority.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 9 July 2019

Contents

1	Summary of the Facts	4
2	Assessment	5
2.1	General reasoning of the Board regarding the submitted draft decision	5
2.2	Analysis of the draft decision (composed of the explanatory notes and the ordinance)	6
2.2.1	INDEPENDENCE.....	6
2.2.2	CONFLICT OF INTEREST.....	8
2.2.3	EXPERTISE	9
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES.....	10
2.2.5	TRANSPARENT COMPLAINTS HANDLING	10
2.2.6	COMMUNICATION WITH THE COMPETENT SUPERVISORY AUTHORITY	11
2.2.7	REVIEW MECHANISMS.....	12
2.2.8	LEGAL STATUS.....	12
3	Conclusions / Recommendations	13
4	Final Remarks	15

The European Data Protection Board

Having regard to article 63, article 64 (1)(c), (3) - (8) and article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to article 10 and 22 of its Rules of Procedure of 25 May 2018, as amended on 23 November 2018

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the Board) is to ensure the consistent application of the GDPR when a supervisory authority (SA) intends to approve the requirements for accreditation of a code of conduct (hereinafter "code") monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting competent supervisory authorities to draft their requirements for accreditation of monitoring bodies based on the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines"), using the eight requirements as outlined in the guidelines' accreditation section (section 12); secondly, to provide written guidance explaining the accreditation requirements; and finally by requesting them to adopt these requirements in line with this opinion so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies), must be identified as part of the code and accredited by the competent supervisory authority as being capable of effectively monitoring the code. The GDPR does not define the term 'accreditation'. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements which should be met in

order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Austrian Supervisory Authority (AT SA) has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board via the IMI system requesting an opinion from the Board pursuant to article 64 (1)(c) for a consistent approach at Union level. The decision on the completeness of the file was taken on 9th of April 2019.
2. The draft accreditation requirements of code monitoring bodies were provided by the AT SA in an English version although they were originally drafted in German. The Board hereby gives its opinion on the English version of the draft accreditation requirements recommending the AT SA to amend and align both versions in accordance with the present opinion.

3. In compliance with article 10 (2) of the Board Rules of Procedure¹, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks, until the 16th of July 2019.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft decision

4. All accreditation requirements submitted to the Board for an opinion must fully address article 41(2) GDPR criteria and be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
5. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1)(p) GDPR, all the SAs will cover these basic core requirements foreseen in the Guidelines, and the Board will recommend that the SAs amend their drafts accordingly to ensure consistency.
6. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request supervisory authorities, the Board and the Commission to ‘encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.’ (article 40 (1) GDPR). Therefore the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
7. In some areas the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for illustrative purposes only. Therefore the encouragements and the examples provided in the present opinion do not have to be followed. However, the aim of these examples is to help the AT SA to further develop consistent accreditation requirements in line with the present opinion.
8. When this opinion remains silent on a specific requirement, it means that the Board is not asking the AT SA to take further action.
9. The Board notes that the document submitted by AT SA is a draft decision on the accreditation requirements for monitoring bodies consisting of two parts:
 - 1) “Explanatory notes” which contain general and specific explanations.

¹ Version 2, as last modified and adopted on 23 November 2018

- 2) The “Ordinance” which sets out the AT accreditation requirements.
10. This opinion does not reflect upon items submitted by the AT SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR where required.

2.2 Analysis of the draft decision (composed of the explanatory notes and the ordinance)

11. Taking into account that:
- Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation;
 - Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited,

the Board is of the opinion that:

2.2.1 INDEPENDENCE

12. With regard to section three of the AT SA’s ordinance, the Board highlights that the obligation to provide evidence as to the independence of a monitoring body falls upon the body applying for accreditation (see article 41 (2)(a) GDPR). The Board recommends that this is clarified in the AT SA’s requirements.
13. The Board observes that the AT SA’s explanatory notes, ‘general notes’ section concerning the requirements, refer to independence *“in relation to the subject matter of the code”*. The Guidelines provide further information about what this means, i.e. the independence of the body concerned should be demonstrated in relation to the code members, the profession, industry or sector to which the code applies and the code owner itself. Therefore, the Board recommends that the AT SA redraft this reference in line with the Guidelines.
14. The Board is of the opinion that independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. These rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, nor subject to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself.

15. Where the monitoring body is part of the code owner organisation, particular focus must be made on their ability to act independently. Examples of internal monitoring bodies could include an ad hoc internal committee or a separate department within the organisation of the code owner. Rules and procedures have to be established to ensure that such a “committee” acts autonomously and without any pressure from the code owner or the code members.
16. The Board notes that the AT SA’s requirements make no reference to the two main models of monitoring, as identified in the Guidelines. The Board therefore recommends that the AT SA amend the requirements to reflect this flexibility. One option would be to require that an internal monitoring body provides evidence of additional measures, to ensure that the relationship with the legal entity (of which the monitoring body is part of), does not compromise the independence of its monitoring activities.
17. The Board observes that a specific provision of the draft accreditation requirements submitted by AT SA is devoted to the demonstration of independence by the monitoring body (section 3.2 of the AT ordinance). The said provision asks for information on persons authorised to make decisions, showing that there are no personal ties with the entities to be monitored. In addition, the explanatory note concerning the independence requirements clarifies that the monitoring body shall not be legally, economically, personally or professionally subordinate to or in close relationship with the monitored entities, which could bring into question its judgement or its independence and integrity in its function as a monitoring body.
18. The Board is of the opinion that the accreditation requirements should qualify what constitutes independence and clearly set out the areas where the monitoring body should demonstrate independence. In this regard, the Board recommends that the AT SA further strengthens the independence section in line with the four areas set out below.

1) LEGAL AND DECISION MAKING PROCEDURES

19. The legal form and arrangement of the monitoring body must shield the monitoring body from undue influence from members of the code or code owner which might affect the monitoring of compliance of a code. For instance, the duration, or expiration of the mandate of the monitoring body should be fixed in such a way as to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely affects the independence in carrying out the monitoring activities by the monitoring body.
20. The decision making procedure set out by a monitoring body must also preserve its autonomy and independence. For instance, a monitoring body needs to be able to act independently in its choice and application of sanctions against a controller or processor adhering to the code.

2) FINANCIAL

21. Monitoring bodies should be provided with the financial stability and resources necessary for the effective performance of their tasks as well as be able to manage their budget independently. The means by which the monitoring body obtains financial support (for example, a fee paid by the

members of the code of conduct) should not adversely affect the independence of its task of monitoring compliance of a code.

22. For instance, the monitoring body would not be considered to be financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body.

3) ORGANISATIONAL

23. Monitoring bodies should have the human and technical resources necessary for the effective performance of their tasks. Monitoring bodies should be composed of an adequate number of personnel so that they are able to fully carry out the monitoring functions, reflecting the sector concerned and the risks of the processing activities addressed by the code of conduct. Personnel of the monitoring body shall be responsible and shall retain authority for their decisions regarding the monitoring activities. These organisational aspects could be demonstrated through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel, as well as the duration of the personnel's mandate, contract or other formal agreement with the monitoring body.

4) ACCOUNTABILITY

24. The monitoring body should be able to demonstrate "accountability" for its decisions and actions in order to be considered to be independent. This could be accomplished through such things as setting out the roles and decision making framework and its reporting procedures.

2.2.2 CONFLICT OF INTEREST

25. The Board observes that the AT SA's accreditation requirements do not address conflicts of interest. The Board recommends that the AT SA add requirements covering procedures to avoid conflicts of interest. Such procedures are likely to involve a risk based approach and will vary depending on the code. Risks may arise from the activities or the relationships of the monitoring body and of its personnel.
26. An example of a conflict of interest would be monitoring body personnel investigating complaints against the organisation that they work for. In order to avoid any conflict of interest, the personnel would declare their interest and the work would be reallocated.
27. The Board encourages the AT SA to consider the following practical examples of accreditation requirements:
 - A monitoring body shall identify situations that are likely to create a conflict of interest (due to its personnel, its organisation, its procedures, etc.) and set up internal rules in order to avoid conflicts of interest.

- A monitoring body shall provide a procedure to deal with the effects of situations identified as being likely to create a conflict of interest.
- Monitoring body personnel must commit in writing to complying with this requirement and to report any situation likely to create a conflict of interest and follow the procedures to avoid such conflicts.
- A monitoring body shall identify and eliminate risks to its impartiality on an ongoing basis. Evidence will include its risk management approach and associated procedures.

2.2.3 EXPERTISE

28. The Board notes that the AT SA's expertise requirements include: an excellent knowledge of data protection and either a relevant degree (or equivalent qualification), or at least five years of relevant sector experience, which may include a maximum of two years of professional activity in an area other than the subject matter of the code (sections 3.4 and 3.5 of the AT ordinance).
29. The Board acknowledges that the guidelines set a high bar requiring monitoring bodies to have the following expertise: an in-depth understanding of data protection issues, knowledge of the specific processing activities in relation to the code and appropriate operational experience and training for monitoring, such as auditing.
30. The Board considers that the accreditation requirements need to be transparent. They also need to provide for monitoring bodies seeking accreditation in relation to codes that cover micro, small and medium-sized enterprises' processing activities (article 40 (1) GDPR).
31. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (in section 6.4 of the Guidelines), by demonstrating 'why their proposals for monitoring are appropriate and operationally feasible' (paragraph 41, page 17 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code's monitoring activities effectively. This could include taking into account such factors as: the size of the sector concerned, the different interests involved and the risks of the processing activities addressed by the code. This is without prejudice to data protection requirements. This would also be important if there are several monitoring bodies, as the code will help ensure a uniform application of the expertise requirements for all monitoring bodies covering the same code.
32. The Board encourages the AT SA to take into account the additional expertise requirements that can be defined by the code and ensure that the expertise of each monitoring body is assessed in line with the particular code. Whereby the SA will verify if the monitoring body possess adequate competencies for the specific duties and responsibilities to undertake the effective monitoring of the code.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

33. The Board observes that section 4 of the ordinance is too general. The Board is of the opinion that the procedures to monitor compliance with codes of conduct have to be specific enough to ensure a consistent application of the obligations of code monitoring bodies.
34. The procedures need to address the complete monitoring process, from the preparation of the evaluation to the conclusion of the audit and additional controls to ensure that appropriate actions are taken to remedy infringements and to prevent repeated offences.
35. The monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear time frame, and check eligibility of members prior to joining the code.
36. Moreover, monitoring body personnel shall keep confidential all information obtained or created during the performance of the monitoring activities, except as required by law.
37. The Board encourages the AT SA to consider the following examples of procedures:
 - A procedure that provides for audit plans, to be carried out over a defined period of time (initial control and recurring controls), based on criteria such as the number of adherents to the code of conduct, the geographical scope, the received complaints, etc.
 - An audit procedure that defines the audit methodology to be applied, i.e. a set of criteria to be assessed (common evaluation grid), the type of audit (self-assessment, off-site or on- site audits, ISO auditing standards), the documentation of the findings, etc.
 - A procedure for the investigation, identification and management of infringement to the code that applies, when required, penalties as defined by the code of conduct (a penalty matrix)
38. The Board recommends that optional requirements regarding monitoring procedures are provided in the AT explanatory notes and that mandatory requirements are clarified in the AT ordinance.
39. The Board recommends that the objectives for each required procedure are explicitly defined in the accreditation requirements.
40. The Board recommends that the reference to “relevant certificates” - that occurs more than once in the AT draft accreditation requirements - is clarified.

2.2.5 TRANSPARENT COMPLAINTS HANDLING

41. With regard to the complaints handling procedure, the Board observes that the AT SA accreditation requirements (section 5.3.4 of the AT SA’s ordinance) include the duration of the proceedings, stating that “it should in any event not exceed two months from the date of receipt of the complaint”.
42. The Board recommends that complaints handling process requirements should be set at a high level and reference reasonable time frames for answering complaints. An example of a reasonable time

period could be that the complainant should be notified within three months on the progress or outcome of the complaint (similar to article 78 (2) GDPR). The process should be: documented, independent, effective and transparent, in order to ensure trust in the code. Accessible complaints procedures should be covered in the code itself. The complaints handling process should be accessible by data subjects and the public.

43. The Board encourages the AT SA to consider the following practical examples of requirements:
 - A monitoring body shall provide evidence of how it will manage complaints procedures and explain time frames.
 - A monitoring body shall outline a procedure to receive, manage and process complaints. This procedure must be independent and transparent.
 - The complaints procedure shall be publicly available and easily accessible.
 - The procedure shall ensure that all complaints are processed within a reasonable period of time.
 - A monitoring body shall maintain a record of all complaints it receives and the actions taken, which the SA can access at any time.

2.2.6 COMMUNICATION WITH THE COMPETENT SUPERVISORY AUTHORITY

44. The Board notes that the AT SA's ordinance, section 6.4 provides for annual reporting by the monitoring body to the Competent Supervisory Authority (hereinafter the CSA). The Board recommends that AT SA amend section 6.4 of the ordinance, in order to provide for more regular communication means to the CSA during the year.
45. The Board is of the opinion that the requirements need to address such areas as: actions taken in cases of infringement of the code and the reasons for taking them (article 41 (4) GDPR), periodic reports, reviews or audit findings. The code itself will also outline the communication requirements with the CSA, including appropriate ad hoc and regular reports. In the case of serious infringements of the code by code members, which result in serious actions such as suspension or exclusion from the code, the competent SA should be informed without delay.
46. The Board considers 'substantial change' to cover any change that impacts on the monitoring body's ability to perform its function independently and effectively. A substantial change would trigger a re-accreditation or new accreditation process. The Board recommends that the AT SA address the reporting of any substantial change to the CSA in the accreditation requirements.
47. The Board encourages the AT SA to consider the following practical examples of requirements:
 - A monitoring body shall set out reporting mechanisms.
 - A monitoring body shall inform the CSA, without undue delay, of any substantial change to the monitoring body (particularly relating to structure or organisation) which is likely to call into

question its independence, expertise and the absence of any conflict of interests or to adversely affect its full operation.

2.2.7 REVIEW MECHANISMS

48. The Board is of the opinion that the monitoring body has a key role in contributing to the review of the code and shall apply code updates (amendment or extension of the code) as decided by the code owner.
49. The Board encourages accreditation requirements which require a monitoring body to develop mechanisms that enable feed back to the code owners. Some options would be to use the results of the audit process, the handling of complaints or actions taken in code infringement cases.
50. For instance, records of the processing of complaints (received and treated), infringements and remedies can be a good way to centralise relevant information in order to develop improvements to the code
51. The Board encourages the AT SA to provide accreditation requirements which will ensure that the monitoring body will contribute to any review of the code, in accordance with the code owner's instructions.

2.2.8 LEGAL STATUS

52. The Board observes that section 2.2 of the AT SA's ordinance provides that a monitoring body may be based outside of the EEA. The Board is of the opinion that a monitoring body requires an establishment in the EEA. This is to ensure that they can uphold data subject rights, deal with complaints and that GDPR is enforceable and also ensures supervision by the CSA. The Board recommends that AT SA require that the monitoring body has an establishment in the EEA
53. Furthermore, the Board observes that the AT SA draft requirements do not provide for the accreditation of monitoring bodies in relation to codes that are approved as a tool for international transfers, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards (article 46 (2)(e) GDPR). In this regard, it is worth noting that supplementary requirements may need to be added, once guidelines for codes as a means of facilitating international transfers have been adopted by the Board.
54. The Board observes that the AT SA's explanatory note for section 2.1 clarifies that natural persons can be accredited as a monitoring body. The Board encourages the AT SA to provide additional requirements in order for such a monitoring body to be accredited. These would include: being able to demonstrate the availability of adequate resources for the specific duties and responsibilities, as well as the full operation of the monitoring mechanism over time. Examples of scenarios to consider include: in the case of resignation or temporary inability of the person concerned.

- 55. The Board recommends that the AT SA require that the monitoring body should have access to adequate resource requirements to fulfil its monitoring responsibilities, especially for the accreditation of a natural person as a monitoring body.
- 56. Moreover, the code of conduct itself will need to demonstrate that the operation of the code's monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that a monitoring body demonstrates that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. Therefore, the Board recommends AT SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.
- 57. The Board is of the opinion that a monitoring body does not need to have a specific legal form to apply for accreditation, provided that it can be held legally responsible for all its monitoring activities and demonstrate sufficient resources to deliver its monitoring functions (for example, effectiveness of administrative fines, etc.).
- 58. Finally, the Board notes that the AT SA's explanatory notes and ordinance do not reference subcontracting, leaving this area open for monitoring bodies applying for accreditation to decide upon. The Board recommends that AT SA clarifies whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the explanatory notes or ordinance accordingly. If AT SA indicates that subcontracting is allowed, the Board recommends that the AT SA indicates, in its ordinance, that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

3 CONCLUSIONS / RECOMMENDATIONS

- 59. The draft accreditation requirements of the Austrian Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
- 60. Regarding 'independence' the Board recommends that the AT SA:
 1. clarify that the task of providing evidence as to the independence of a monitoring body to the satisfaction of a CSA falls upon the body applying for accreditation;
 2. redraft the explanatory note reference to "in relation to the subject matter of the code", so that it is in line with the Guidelines;
 3. amend the requirements to reflect the two models of monitoring bodies set out in the Guidelines; and
 4. strengthen its requirements in line with the four areas (legal and decision making, financial, organisational and accountability) in order to qualify what constitutes independence.
- 61. Regarding 'conflict of interest' the Board recommends that the AT SA:
 - adopted

1. add requirements covering procedures to avoid conflicts of interest.
62. Regarding ‘established procedures and structures’ the Board recommends that the AT SA:
 1. provide optional requirements regarding monitoring procedures in the AT explanatory notes and clarify mandatory requirements in the AT ordinance;
 2. explicitly define the objectives of each required procedure in the accreditation requirements; and
 3. clarify the reference to “relevant certificates”- that occurs more than once in the AT draft accreditation requirements.
63. Regarding ‘transparent complaints handling’ the Board recommends that the AT SA’s:
 1. complaints handling process requirements are set at a high level and reference reasonable time frames for answering complaints.
64. Regarding ‘communication with the competent supervisory authority’ the Board recommends that the AT SA:
 1. amend section 6.4 of the ordinance to provide for more regular communication with the CSA during the year; and
 2. address the reporting of any substantial change to the CSA in the accreditation requirements.
65. Regarding ‘legal status’ the Board recommends that the AT SA:
 1. require that the monitoring body has an establishment in the EEA;
 2. require that the monitoring body should have access to adequate resource requirements to fulfil its monitoring responsibilities and demonstrate that it can deliver the code’s monitoring mechanism over a suitable period of time, especially for the accreditation of a natural person as a monitoring body; and
 3. clarify whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the explanatory notes or ordinance accordingly. If subcontracting is allowed, amend the ordinance, so that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

4 FINAL REMARKS

66. This opinion is addressed to the Austrian supervisory authority and will be made public pursuant to article 64 (5b) GDPR.
67. According to article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 10/2019 on the draft list of the competent
supervisory authority of Cyprus
regarding
the processing operations subject to the requirement of a
data protection impact assessment (Article 35(4) GDPR)**

Adopted on 9 July 2019

Table of contents

1.	Summary of the Facts.....	4
2.	Assessment.....	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list	6
2.3	Analysis of the draft list.....	6
	REFERENCE TO THE GUIDELINES	6
	MONITORING EMPLOYEES	6
	BIOMETRIC AND GENETIC DATA.....	6
	LOCATION DATA	7
3.	Conclusions / Recommendations.....	7
4.	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64(1)(a), (3) - (8) and Article 35(1), (3), (4), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, as revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereinafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations subject to the requirement for a data protection impact assessment pursuant to Article 35(4) GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by requesting SAs to include some types of processing in their lists, secondly by requesting them to remove some criteria which the Board doesn't consider as necessarily creating high risks for data subjects, and finally by requesting them to use some criteria in a harmonized manner.

(2) With reference to Article 35(4) and (6) GDPR, the competent supervisory authorities shall establish lists of the kind of processing operations which are subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects.

(4) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35(1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 35 (3) GDPR illustrates what is likely to result in a high risk. This is a non-exhaustive list. The Working Party 29 in the Guidelines on data protection impact assessment¹, as endorsed by the EDPB², has clarified criteria that can help to identify when processing operations are subject to the requirement for a DPIA. The Working Party 29 Guidelines

WP248 state that in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out, however, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(5) The lists produced by the competent supervisory authorities support the same objective to identify processing operations likely to result in a high risk and processing operations, which therefore require a DPIA. As such, the criteria developed in the Working Party 29 Guidelines should be applied when assessing whether the draft lists of the competent supervisory authorities does not affect the consistent application of the GDPR.

(6) Twenty-two competent supervisory authorities received an opinion on their draft lists from the EDPB on 5 September 2018. A further 4 SAs received an opinion on their draft lists on 4 December 2018, followed by 2 on 23 January 2019 and another 2 on 12 March 2019. A global assessment of these draft lists supports the objective of a consistent application of the GDPR.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1. Summary of the Facts

1. The Office of the Commissioner of Personal Data Protection in Cyprus (hereafter Cypriot Supervisory Authority) has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 5 April 2019. The period until which the opinion has to be adopted has been extended until 12 July 2019.

¹ WP29, Guidelines on Data Protection Impact Assessment and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (WP 248 rev. 01).

² EDPB, Endorsement 1/2018.

2. Assessment

2.1 General reasoning of the EDPB regarding the submitted list

2. Any list submitted to the EDPB has been interpreted as further specifying Art 35(1), which will prevail in any case. Thus, no list can be exhaustive.
3. In compliance with Article 35(10) GDPR, the Board is of the opinion that if a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of the legal basis the obligation to carry out a DPIA in accordance with paragraphs 1 to 7 of Article 35 GDPR does not apply, unless the Member State deems it necessary.
4. Further, if the Board requests a DPIA for a certain category of processing and an equivalent measure is already required by national law, the Cypriot Supervisory Authority Protection shall add a reference to this measure.
5. This opinion does not reflect upon items submitted by the Cypriot Supervisory Authority, which were deemed outside the scope of Article 35(6) GDPR. This refers to items that neither relate “to the offering of goods or services to data subjects” in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to “substantially affect the free movement of personal data within the Union”. This is especially the case for items relating to national legislation and in particular, where the obligation to carry out a DPIA is stipulated in national legislation. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
6. The Board has noted that several supervisory authorities have included in their lists some types of processing which are necessarily local processing. Given that only cross border processing and processing that may affect the free flow of personal data and data subjects are concerned by Article 35(6), the Board will not comment on those local processing.
7. The opinion aims at defining a consistent core of processing operations that are recurrent in the lists provided by the SAs.
8. This means that, for a limited number of types of processing operations that will be defined in a harmonised way, all the Supervisory Authorities will require a DPIA to be carried out and the Board will recommend the SAs to amend their lists accordingly in order to ensure consistency.
9. When this opinion remains silent on DPIA list entries submitted, it means that the Board is not asking the Cypriot Supervisory Authority to take further action.
10. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists, for each type of processing, to the criteria set out in the guidelines could improve this transparency. Therefore, the Board considers that an explanation on which criteria have been taken into account by the Cypriot Supervisory Authority to create its list could be added.

2.2 Application of the consistency mechanism to the draft list

11. The draft list submitted by the Cypriot Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

12. Taking into account that:
 - a. Article 35(1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35(3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

13. The board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 is a core element for ensuring consistency across the Union. Thus, it requests the different Supervisory Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.
14. As the document of the Cypriot Supervisory Authority does not contain such a statement, the Board recommends the Office of the Commissioner of Personal Data Protection to amend their document accordingly.

MONITORING EMPLOYEES

15. The Board is of the opinion that, due to its specific nature, the employee monitoring processing, meeting the criterion of vulnerable data subjects and of systematic monitoring in the guidelines, – could require a DPIA. Given that the list submitted by the Cypriot Supervisory Authority for an opinion of the Board already envisages this type of processing as requiring a data protection impact assessment, the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248. In addition, the Board is of the opinion that the WP249 of the Article 29 working party remains valid when defining the concept of the systematic processing of employee data.

BIOMETRIC AND GENETIC DATA

16. The list submitted by the Cypriot Supervisory Authority for an opinion of the Board envisages that the large-scale processing of “biometric and genetic data” requires a DPIA. On this point, the Board acknowledges that the list aligns with the aim of consistency. However, the Board notes that the phrasing used might lead to the conclusion that the large scale processing of biometric data must take place cumulatively with genetic data, whereas it should be a disjunctive condition. Therefore, the Board recommends that the phrasing be changed to ‘biometric or genetic data’.

LOCATION DATA

17. The Board is of the opinion that consistency is one of the basic principles of the GDPR. The Board notes that a majority of the lists submitted explicitly contain a reference to the processing of location data. As the list submitted by the Cypriot Supervisory Authority for an opinion does not contain such a reference, the Board encourages the Cypriot Supervisory Authority to include the processing of location data in its list, together with another criterion.

3. Conclusions / Recommendations

18. The draft list of the Cypriot Supervisory Authority may lead to an inconsistent application of the requirement for a DPIA and the following changes need to made:
 -) Regarding the reference to the guidelines: the Board requests the Supervisory Authority of Cyprus to amend its document accordingly.
 -) Regarding employee monitoring: the Board solely recommends making explicit the reference to the two criteria in the guidelines WP29 Guidelines WP248.
 -) Regarding ‘biometric and genetic data’: the Board recommends that the phrasing be changed to ‘biometric or genetic data’.
 -) Regarding location data: the Board encourages the Cypriot Supervisory Authority to include the processing of location data in its list, together with another criterion.

4. Final Remarks

19. This opinion is addressed to The Office of the Commissioner of Personal Data Protection in Cyprus (Cypriot Supervisory Authority) and will be made public pursuant to Article 64(5)(b) GDPR.
20. According to Article 64(7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 11/2019 on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)

Adopted on 10 July 2019

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list.....	5
2.3	Analysis of the draft list.....	5
	Reference to the guidelines.....	6
	Accounting, Human Resources, and Social and Health Insurance Processing	6
	Processing Related to Business Activities.....	6
	Processing operations consisting in direct marketing	6
	Processing involving the taking of footage by a camera installed on a vehicle	6
	Significance of the items on the 35(5) GDPR list	6
2.4	List items considered out of scope of Article 35(6) GDPR.....	7
3	CONCLUSIONS / RECOMMENDATIONS	7
4	FINAL REMARKS.....	8

The European Data Protection Board

Having regard to Article 63, Article 64(2) and Article 35(1), (5), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to Article 51(1)(b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereinafter GDPR) throughout the European Economic Area. In compliance with Articles 35(6) and 64(2) GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations not subject to the requirement for a data protection impact assessment pursuant to Article 35(5) GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions by ensuring that the lists do not contradict the cases where the GDPR explicitly states that a type of processing should undergo a DPIA, by recommending SAs to remove some criteria which, the Board considers not correlated with the absence of likelihood of high risks for data subjects, by recommending them to limit the scope of the types of processing in order not to contradict the general rules defined in the DPIA guidelines from the Article 29 Working Party, endorsed by the EDPB, and finally by recommending them to use some criteria in a harmonized manner.

(2) With reference to Article 35(5) and (6) GDPR, the competent supervisory authorities may establish lists of the kind of processing operations which are not subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects across the EEA.

(5) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35(1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. The national SAs can issue lists concerning certain processing activities which always require a DPIA (blacklists) per Article 35(4) as well as lists where no DPIA is necessary per Article 35(5) (whitelists). When a processing does not fall within either of these two lists and is not mentioned Article 35(3) GDPR, an ad hoc decision will have to be made by the data controller based on whether the “likely to result in a high risk to the rights and freedoms of natural persons” criterion is met. According to Recital 91 of the GDPR a DPIA will not be mandatory when the processing is carried out by an individual physician, other health care professional or a lawyer, as it is not of a sufficient large scale. This exception covers only partially the cases when a DPIA will not be necessary, i.e. when there is no high risk to the rights and freedoms of natural persons.

(6) The lists produced by the competent supervisory authorities support a common objective, namely to identify the kind of processing operations for which the national SAs are certain that, under no circumstances, they will result in a high risk, and processing operations the national SAs deem unlikely to result in a high risk, and therefore do not require a DPIA. The Board refers to the Working Party 29 Guidelines on DPIA (WP248 rev.01)¹, which sets out criteria to consider in determining processing operations “*likely to result in a high risk*”.² As set out in these guidelines, in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of the Czech Republic has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 10 April 2019.
2. The period until which the opinion has to be adopted has been extended until 17 July 2019.

¹ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017 and revised on 4 October 2017

² Recitals 75, 76, 92, 116 GDPR.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying on the one hand Article 35 GDPR, which will prevail in any case, and on the other hand recital 91. Thus, no list can be exhaustive.
4. This opinion does not reflect upon items submitted by the Czech Supervisory Authority, which were deemed outside the scope of Article 35(6) GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". However, for the sake of clarity, the Board will enumerate the items of the list, which were deemed outside the scope of Article 35(6) GDPR. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
5. This opinion will not comment on any items on the list, which fall within the scope of recital 91.
6. The opinions on the Article 35(4) GDPR lists also aimed at defining a consistent core of processing operations, which the Board requested all Supervisory Authorities to add to their list if not already present in order to ensure consistency. The Article 35(5) GDPR lists may not exempt these general processing operations as a rule.
7. The lists established by SAs pursuant to Article 35(5) GDPR are inherently non-exhaustive. These lists contain types of processing regarding which national SAs are certain that, under no circumstances, they will result in a high risk to the rights and freedom of natural persons, and processing operations the national SAs deem unlikely to result in a high risk. Such lists cannot enumerate all cases in which a DPIA will not be necessary. In any event, the obligation of the controller or processor to assess the risk of the processing and to comply with the other obligations imposed by the GDPR remain applicable.
8. When this opinion remains silent on an item from the list, it means that the Board is not asking the Czech Supervisory Authority to take further action.
9. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

10. The draft list submitted by the Czech Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

11. Taking into account that:
 - a. Article 35(1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35(3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

12. The Board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 is a core element for ensuring consistency across the Union. Thus, it recommends the different Supervisory Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

ACCOUNTING, HUMAN RESOURCES, AND SOCIAL AND HEALTH INSURANCE PROCESSING

13. The Board notes that the processing of accounting, human resources (HR), and social and health insurance data is a broad item that might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. The Board recommends that the processing activities envisaged by the Czech Supervisory Authority's DPIA list be restricted to processing which is not large scale and is mandatory by law.

PROCESSING RELATED TO BUSINESS ACTIVITIES

14. The Board notes that the processing related to business activities is a broad item that might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. For this reason, the Board recommends that the Czech Supervisory Authority reduces the scope of this item by covering only business-to-customers relations, excluding the processing of sensitive data or data of highly personal nature and by excluding data processing on a large scale.

PROCESSING OPERATIONS CONSISTING IN DIRECT MARKETING

15. The Board notes that "processing operation consisting in direct marketing including customer profiling based on customer choice of items or displayed items for the catalogue of offered goods, products and services posted at the controller's website made during one single visit by a customer" is a broad description that includes processing likely to pose a high risk to the rights and freedoms of natural persons. For this reason, the Board recommends that the Czech Supervisory Authority limit the scope of this item by explicitly excluding the processing of special categories of data and data of a highly personal nature, and by excluding processing that targets vulnerable data subjects deliberately.

PROCESSING INVOLVING THE TAKING OF FOOTAGE BY A CAMERA INSTALLED ON A VEHICLE

16. The Board notes, that processing consisting of the "taking footage by camera installed on a vehicle which monitors a necessary range in front of or behind the vehicle for the purpose of securing documentation of traffic accident and its investigation by competent authorities" might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. For this reason, the Board recommends that the Czech Supervisory Authority remove this item from its list.

SIGNIFICANCE OF THE ITEMS ON THE 35(5) GDPR LIST

17. The Board notes that the mere fact that processing activity falls within the scope of a 35(5) GDPR list does not mean that a controller is exempt from the general obligations of the GDPR. Hence, an assessment of the risks for the rights and freedoms of natural persons, their likelihood and severity, needs to be undertaken by the controller and processor in order to ensure a level of security appropriate to the risk in compliance with Article 32 GDPR. For the sake of clarity, the Board encourages the Czech Supervisory Authority to include in its list a paragraph that mentions the distinction in the application of Articles 32 and 35 of the GDPR.

2.4 List items considered out of scope of Article 35(6) GDPR

18. The Board is of the view that the following item on the list falls outside the scope of Article 35(6) GDPR:¹
 -) processing operation or set of processing operations regulated by law, on condition that a DPIA has been done within the process of a general assessment of impacts of the intended piece of legislation and the processing operation is not incorporated into a common system of the controller and interconnected with other processing operations carried out by the same controller;
19. Therefore, the Board does not have any comments on this item.

3 CONCLUSIONS / RECOMMENDATIONS

20. The draft list of the Czech Supervisory Authority may lead to an inconsistent application of Article 35 GDPR and the following changes need to be made:
 -) Regarding the reference to the guidelines: the Board recommends the Supervisory Authority of the Czech Republic to amend its document accordingly.
 -) Regarding Accounting, HR, and Social and Health Insurance Processing: The Board recommends that the processing activities envisaged by the Czech Supervisory Authority's DPIA list are restricted to processing which are not large scale and are mandatory by law.
 -) Regarding processing Related to Business Activities: the Board recommends that this item be amended to restrict the scope to business-to-customers only and to exclude the processing of sensitive data or data of a highly personal nature, and to exclude large scale processing.
 -) Regarding processing operations consisting in direct marketing: the Board recommends that this item be amended to restrict the scope by excluding processing of special categories of data and data of a highly personal nature, as well as processing deliberately targeting vulnerable subjects as a specific group.
 -) Regarding processing involving the taking of footage by a camera installed on a vehicle: the Board recommends that the Czech Supervisory Authority remove this item from its list.
 -) Regarding the significance of items listed: the Board encourages the Czech Supervisory Authority to clarify that its list is without prejudice to any other obligation stipulated by the GDPR.

¹ This view is strictly tied to the present list and does not apply necessarily to similar items in the lists submitted by other Supervisory Authorities.

4 FINAL REMARKS

21. This opinion is addressed to the Úřad pro ochranu osobních údajů (Czech Supervisory Authority) and will be made public pursuant to Article 64(5)(b) GDPR.
22. The Czech Supervisory Authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 12/2019 on the draft list of the competent supervisory authority of Spain regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)

Adopted on 10 July 2019

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list.....	5
2.3	Analysis of the draft list.....	5
	Reference to the guidelines.....	6
	Processing under guidelines established by or previously authorised by supervisory bodies	6
	Processing under the guidelines of codes of conduct.....	6
	Processing carried out to comply with a legal requirement or to complete a mission	6
	Processing of human resources, accounting, and social security data by SMEs.....	6
	Processing by Professional Colleges and Non-Profit Associations	6
	Processing to protect the vital interests of the data subject	6
	Significance of the items on the 35.5 GDPR list	7
2.4	List items considered out of scope of Article 35(6) GDPR.....	7
3	CONCLUSIONS / RECOMMENDATIONS.....	7
4	FINAL REMARKS.....	8

The European Data Protection Board

Having regard to Article 63, Article 64(2) and Article 35(1), (5), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to Article 51(1)(b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereinafter GDPR) throughout the European Economic Area. In compliance with Articles 35(6) and 64(2) GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations not subject to the requirement for a data protection impact assessment pursuant to Article 35(5) GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions by ensuring that the lists do not contradict the cases where the GDPR explicitly states that a type of processing should undergo a DPIA, by recommending SAs to remove some criteria which, the Board considers not correlated with the absence of likelihood of high risks for data subjects, by recommending them to limit the scope of the types of processing in order not to contradict the general rules defined in the DPIA guidelines from the Article 29 Working Party, endorsed by the EDPB, and finally by recommending them to use some criteria in a harmonized manner.

(2) With reference to Article 35(5) and (6) GDPR, the competent supervisory authorities may establish lists of the kind of processing operations which are not subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects across the EEA.

(5) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35(1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. The national SAs can issue lists concerning certain processing activities which always require a DPIA (blacklists) per Article 35(4) as well as lists where no DPIA is necessary per Article 35(5) (whitelists). When a processing does not fall within either of these two lists and is not mentioned Article 35(3) GDPR, an ad hoc decision will have to be made by the data controller based on whether the “likely to result in a high risk to the rights and freedoms of natural persons” criterion is met. According to Recital 91 of the GDPR a DPIA will not be mandatory when the processing is carried out by an individual physician, other health care professional or a lawyer, as it is not of a sufficient large scale. This exception covers only partially the cases when a DPIA will not be necessary, i.e. when there is no high risk to the rights and freedoms of natural persons.

(6) The lists produced by the competent supervisory authorities support a common objective, namely to identify the kind of processing operations for which the national SAs are certain that, under no circumstances, they will result in a high risk, and processing operations the national SAs deem unlikely to result in a high risk, and therefore do not require a DPIA. The Board refers to the Working Party 29 Guidelines on DPIA (WP248 rev.01)¹, which sets out criteria to consider in determining processing operations “likely to result in a high risk”.² As set out in these guidelines, in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of Spain has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 19 June 2019.
2. The period until which the opinion has to be adopted has been extended until 25 September 2019.

¹ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017 and revised on 4 October 2017

² Recitals 75, 76, 92, 116 GDPR.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying on the one hand Article 35 GDPR, which will prevail in any case, and on the other hand recital 91. Thus, no list can be exhaustive.
4. This opinion does not reflect upon items submitted by the Spanish Supervisory Authority, which were deemed outside the scope of Article 35(6) GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". However, for the sake of clarity, the Board will enumerate the items of the list, which were deemed outside the scope of Article 35(6) GDPR. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
5. This opinion will not comment on any items on the list, which fall within the scope of recital 91.
6. The opinions on the Article 35(4) GDPR lists also aimed at defining a consistent core of processing operations, which the Board requested all Supervisory Authorities to add to their list if not already present in order to ensure consistency. The Article 35(5) GDPR lists may not exempt these general processing operations as a rule.
7. The lists established by SAs pursuant to Article 35(5) GDPR are inherently non-exhaustive. These lists contain types of processing regarding which national SAs are certain that, under no circumstances, they will result in a high risk to the rights and freedom of natural persons, and processing operations the national SAs deem unlikely to result in a high risk. Such lists cannot enumerate all cases in which a DPIA will not be necessary. In any event, the obligation of the controller or processor to assess the risk of the processing and to comply with the other obligations imposed by the GDPR remain applicable.
8. When this opinion remains silent on an item from the list submitted, it means that the Board is not asking the Spanish Supervisory Authority to take further action.
9. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

10. The draft list submitted by the Spanish Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

11. Taking into account that:
 - a. Article 35(1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35(3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

12. The Board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 is a core element for ensuring consistency across the Union. Thus, it recommends the different Supervisory Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

PROCESSING UNDER GUIDELINES ESTABLISHED BY OR PREVIOUSLY AUTHORISED BY SUPERVISORY BODIES

13. The Board notes that the item is closely related to recital 171 GDPR and that this issue is dealt with in the WP29 Guidelines on DPIA. However, to ensure clarity, the Board recommends that the Spanish Supervisory Authority clarifies that this exemption is valid only if the processing has not changed since it was authorized.

PROCESSING UNDER THE GUIDELINES OF CODES OF CONDUCT

14. The Board is of the opinion that the processing carried out strictly under guidelines of codes of conduct approved by the Commission or by the supervisory bodies does not by itself lift the obligation to perform a DPIA. Thus, the Board recommends that the Spanish Supervisory Authority specifies that only processing for which a full DPIA has already been carried out within a validated code of conduct, and which are implemented with the measures and safeguards defined in the DPIA, do not require a separate DPIA.

PROCESSING CARRIED OUT TO COMPLY WITH A LEGAL REQUIREMENT OR TO COMPLETE A MISSION

15. The Board is of the opinion that the processing “that is strictly necessary to comply with a legal requirement or to complete a mission being carried out in the public interest, provided that there is no duty to carry out a DPIA within the legal mandate” itself does not by itself lift the obligation to perform a DPIA. Thus, the Board recommends that the Spanish Supervisory Authority restrict the item to situations where the DPIA has already been performed.

PROCESSING OF HUMAN RESOURCES, ACCOUNTING, AND SOCIAL SECURITY DATA BY SMEs

16. The Board notes that the processing of accounting, human resources (HR), and social security data in general is a broad item that might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. The Board recommends that the processing activities envisaged by the Spanish Supervisory Authority’s DPIA list be restricted to processing operations which is mandatory by law.

PROCESSING BY PROFESSIONAL COLLEGES AND NON-PROFIT ASSOCIATIONS

17. The Board notes that the processing of professional colleges and non-profit associations in general is a broad item that might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. The Board recommends that the processing activities envisaged by the Spanish Supervisory Authority’s DPIA list are restricted to processing that concerns exclusively the management of personal data in relation to members and donors of the data controllers listed therein.

PROCESSING TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT

18. The Board notes that this item does not refer to a kind of processing activity but to a legal ground that a data controller can use to justify the lawfulness of its processing. The Board considers that whether

a processing activity is likely to result in a high risk to the rights and freedoms of natural persons depends on the nature and characteristics of that activity and not on the legal ground that deems it lawful. For this reason, the Board recommends that this item be removed from the Spanish Art 35.5 GDPR list.

SIGNIFICANCE OF THE ITEMS ON THE 35.5 GDPR LIST

19. The Board notes that the mere fact that processing activity falls within the scope of a 35.5 GDPR list does not mean that a controller is exempt from the general obligations of the GDPR. Hence, an assessment of the risks for the rights and freedoms of natural persons, their likelihood and severity, needs to be undertaken by the controller and processor in order to ensure a level of security appropriate to the risk in compliance with Article 32 GDPR. For the sake of clarity, the Board encourages to the Spanish Supervisory Authority to include in its list a paragraph that mentions the distinction in the application of Articles 32 and 35 of the GDPR.

2.4 List items considered out of scope of Article 35(6) GDPR

20. The Board is of the view that the following items on the list fall outside the scope of Article 35(6) GDPR:¹

-) Processing carried out by owners' associations and sub-associations in multi-occupancy properties, according as these are defined at Article 2 (a, b, and d) of Law 49/1960 on Horizontal Property.

21. Therefore, the Board does have any comments on this item.

3 CONCLUSIONS / RECOMMENDATIONS

22. The draft list of the Spanish Supervisory Authority may lead to an inconsistent application of Article 35 GDPR and the following changes need to be made:

-) Regarding the reference to the guidelines: the Board recommends the Supervisory Authority of the Spain to amend its document accordingly.
-) Regarding processing under guidelines established by or previously authorised by supervisory bodies: the Board recommends that the Spanish Supervisory Authority clarifies that this exemption is valid only if the processing has not changed since it was authorized.
-) Regarding processing under the guidelines of codes of conduct: the Board recommends that the Spanish Supervisory Authority specifies that only processing for which a full DPIA has already been carried out within a validated code of conduct, and which are implemented with the measures and safeguards defined in the DPIA, do not require a separate DPIA..
-) Regarding processing carried out to comply with a legal requirement or to complete a mission: the Board recommends that the Spanish Supervisory Authority restrict the item to situations where the DPIA has already been performed.
-) Regarding processing of HR, accounting, and social security data by SMEs: the Board recommends that the processing activities envisaged by the Spanish Supervisory Authority's DPIA list are restricted to processing operations which are mandatory by law.
-) Regarding processing by Professional Colleges and Non-Profit Associations: the Board recommends that the processing activities envisaged by the Spanish Supervisory Authority's

¹ This view is strictly tied to the present list and does not apply necessarily to similar items in the lists submitted by other Supervisory Authorities.

DPIA list are restricted to processing that concerns exclusively the management of personal data in relation to members and donors of the data controllers listed therein.

-) Regarding processing to protect the vital interests of the data subject: the Board recommends that this item be removed.
-) Regarding the significance of items listed: the Board encourages the Spanish Supervisory Authority to clarify that its list is without prejudice to any other obligation stipulated by the GDPR

4 FINAL REMARKS

23. This opinion is addressed to the Agencia Española de Protección de Datos (Spanish Supervisory Authority) and will be made public pursuant to Article 64 (5)(b) GDPR.
24. The Spanish Supervisory Authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)

Adopted on 10 July 2019

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
2.1	General reasoning of the EDPB regarding the submitted list	5
2.2	Application of the consistency mechanism to the draft list.....	5
2.3	Analysis of the draft list.....	5
	Reference to the guidelines.....	6
	Processing personal data in the context of Human Resources	6
	Breathalyser tests and tachographs	6
	Managing access controls and work schedules.....	6
	Recovery of debt.....	6
	Significance of the items on the 35(5) GDPR list	7
	List items considered out of scope of article 35(6) GDPR	7
3	CONCLUSIONS / RECOMMENDATIONS	7
4	FINAL REMARKS.....	8

The European Data Protection Board

Having regard to Article 63, Article 64(2) and Article 35(1), (5), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to Article 51(1)(b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018, revised on 23 November 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereinafter GDPR) throughout the European Economic Area. In compliance with Articles 35(6) and 64(2) GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations not subject to the requirement for a data protection impact assessment pursuant to Article 35(5) GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions by ensuring that the lists do not contradict the cases where the GDPR explicitly states that a type of processing should undergo a DPIA, by recommending SAs to remove some criteria which, the Board considers not correlated with the absence of likelihood of high risks for data subjects, by recommending them to limit the scope of the types of processing in order not to contradict the general rules defined in the DPIA guidelines from the Article 29 Working Party, endorsed by the EDPB, and finally by recommending them to use some criteria in a harmonized manner.

(2) With reference to Article 35(5) and (6) GDPR, the competent supervisory authorities may establish lists of the kind of processing operations which are not subject to the requirement for a data protection impact assessment (hereinafter "DPIA"). They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

Adopted

(4) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects across the EEA.

(5) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35(1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. The national SAs can issue lists concerning certain processing activities which always require a DPIA (blacklists) per Article 35(4) as well as lists where no DPIA is necessary per Article 35(5) (whitelists). When a processing does not fall within either of these two lists and is not mentioned Article 35(3) GDPR, an ad hoc decision will have to be made by the data controller based on whether the “likely to result in a high risk to the rights and freedoms of natural persons” criterion is met. According to Recital 91 of the GDPR a DPIA will not be mandatory when the processing is carried out by an individual physician, other health care professional or a lawyer, as it is not of a sufficient large scale. This exception covers only partially the cases when a DPIA will not be necessary, i.e. when there is no high risk to the rights and freedoms of natural persons.

(6) The lists produced by the competent supervisory authorities support a common objective, namely to identify the kind of processing operations for which the national SAs are certain that, under no circumstances, they will result in a high risk, and processing operations the national SAs deem unlikely to result in a high risk, and therefore do not require a DPIA. The Board refers to the Working Party 29 Guidelines on DPIA (WP248 rev.01)¹, which sets out criteria to consider in determining processing operations “likely to result in a high risk”.² As set out in these guidelines, in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of France has submitted its draft list to the EDPB. The decision on the completeness of the file was taken on 20 May 2019.
2. The period until which the opinion has to be adopted has been extended until 26 August 2019.

¹ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017 and revised on 4 October 2017

² Recitals 75, 76, 92, 116 GDPR.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying on the one hand Article 35 GDPR, which will prevail in any case, and on the other hand recital 91. Thus, no list can be exhaustive.
4. This opinion does not reflect upon items submitted by the French Supervisory Authority, which were deemed outside the scope of Article 35(6) GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". However, for the sake of clarity, the Board will enumerate the items of the list, which were deemed outside the scope of Article 35(6) GDPR. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
5. This opinion will not comment on any items on the list, which fall within the scope of recital 91.
6. The opinions on the Article 35(4) GDPR lists also aimed at defining a consistent core of processing operations, which the Board requested all Supervisory Authorities to add to their list if not already present in order to ensure consistency. The article 35(5) GDPR lists may not exempt these general processing operations as a rule.
7. The lists established by SAs pursuant to Article 35(5) GDPR are inherently non-exhaustive. These lists contain types of processing regarding which national SAs are certain that, under no circumstances, they will result in a high risk to the rights and freedom of natural persons, and processing operations the national SAs deem unlikely to result in a high risk. Such lists cannot enumerate all cases in which a DPIA will not be necessary. In any event, the obligation of the controller or processor to assess the risk of the processing and to comply with the other obligations imposed by the GDPR remain applicable.
8. When this opinion remains silent on an item from the list, it means that the Board is not asking the French Supervisory Authority to take further action.
9. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

10. The draft list submitted by the French Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.

2.3 Analysis of the draft list

11. Taking into account that:
 - a. Article 35(1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; and
 - b. Article 35(3) GDPR provides a non-exhaustive list of types of processing that require a DPIA,

the Board is of the opinion that:

REFERENCE TO THE GUIDELINES

12. The Board is of the opinion that the analysis done in the Working Party 29 Guidelines WP248 is a core element for ensuring consistency across the Union. Thus, it recommends the different Supervisory Authorities to add a statement to the document containing their list that clarifies that their list is based on these guidelines and that it complements and further specifies the guidelines.

PROCESSING PERSONAL DATA IN THE CONTEXT OF HUMAN RESOURCES

13. The French list includes the "*Processing operations, implemented under the conditions laid down by the applicable texts, solely for human resources purposes by employers with fewer than 250 people, except when profiling is used*". The Board notes that the processing of personal data in the context of human resources (HR data) is a broad item that might involve categories of personal data, the processing of which is likely to pose a high risk to the rights and freedoms of natural persons. However, the processing activities envisaged by the French Supervisory Authority's list are restricted to processing that are not conducted on a large scale and are mandatory by law. The Board therefore deems this list item in accordance with Article 35(5) GDPR.

BREATHALYSER TESTS AND TACHOGRAPHHS

14. The French list includes "*Processing relating to breathalyser tests and tachographs implemented in the framework of transport activities*". The Board notes that the item concerning processing relating to breathalyzer tests and tachographs is broad and may involve processing which is likely to pose a high risk to the rights and freedoms of natural persons. For this reason, the Board recommends that this item be further restricted to cases where processing of such data is mandatory by law, that the purposes of the use of breathalyzer test data is restricted to the sole purpose of preventing drivers from operating vehicles while under the influence of alcohol or narcotics, and that the use of tachographs, is removed from the list.

MANAGING ACCESS CONTROLS AND WORK SCHEDULES

15. The French list includes the "*Processing carried out solely for the purpose of managing access controls and schedules, excluding any biometric device*". The Board is of the opinion that the processing activities carried out in the context of managing access controls and work schedules is a broad item that might include processing, which are likely to pose a high risk to the rights and freedoms of natural persons. Hence, the Board recommends this item be further restricted to cover only processing of data that does not reveal sensitive data or data of a highly personal nature. With respect to access control, the Board recommends restricting the scope of the item to processing activities solely in the context of standard and non-biometric mechanisms aimed at controlling physical access. Further, the Board recommends clarifying in the item that, with respect to work schedules, only processing activities with the sole purpose of calculating working times are covered.

RECOVERY OF DEBT

16. The French list includes the "*Processing operations carried out by the data controller for the recovery of its outstanding debts, and for its own account*". The Board is of the opinion that the processing activities carried out in the context of recovery of debt is a broad item that may cover processing which is likely to pose a high risk to the rights and freedoms of natural persons. The Board recommends that the French Supervisory Authority further restrict the scope of this item by stating that it does not apply to the processing activities concerning debts which have been acquired from a third party, and that it only applies to debts owed in the context of a business to consumer relationship. Furthermore, the Board recommends that evaluation and scoring be explicitly excluded from scope of this item.

SIGNIFICANCE OF THE ITEMS ON THE 35(5) GDPR LIST

17. The Board notes that the mere fact that processing activity falls within the scope of a 35(5) GDPR list does not mean that a controller is exempt from the obligations set out in Article 32 GDPR. Hence, an assessment of the risks for the rights and freedoms of natural persons, their likelihood and severity, needs to be undertaken by the controller and processor in order to ensure a level of security appropriate to the risk in compliance with Article 32 GDPR. The Board encourages the French Supervisory Authority to include in its list a paragraph making this distinction between Articles 32 and 35 of the GDPR for the sake of clarity.

LIST ITEMS CONSIDERED OUT OF SCOPE OF ARTICLE 35(6) GDPR

18. The Board is of the view that the following items on the list fall outside the scope of Article 35(6) GDPR¹ and consequently does not issue recommendations on these items.
-) Processing implemented under the conditions provided by the law relating to the management of the electoral register of municipalities;
 -) Processing carried out by the clerks of commercial courts for the purpose of carrying out their activity;
 -) Processing carried out by notaries for the purpose of carrying out their notarial activity and the drafting of notarial office documents;
 -) Processing carried out by local authorities, as well as legal persons covered by public and private law, for the management of schools, as well as extracurricular and early childhood services.
19. Therefore, the Board does not have any comments on these items.

3 CONCLUSIONS / RECOMMENDATIONS

20. The draft list of the French Supervisory Authority may lead to an inconsistent application of Article 35 GDPR and recommends that the following changes be made:
-) Regarding the reference to the guidelines: the Board recommends the Supervisory Authority of France to amend its document accordingly.
 -) Regarding breathalyser tests and tachographs: the Board recommends that this item be restricted to processing mandated by law, that it be restricted to the sole purpose of preventing drivers from operating vehicles while under the influence of alcohol or narcotics and that the processing involving the use of a tachograph be removed from the list.
 -) Regarding managing access controls: the Board recommends this item be restricted to cover only processing of data that does not reveal sensitive data or data of a highly personal nature. With respect to access control, the Board recommends restricting the scope of the item to processing activities solely in the context of standard and non-biometric mechanisms aimed at controlling physical access. Further, the Board recommends clarifying in the item that, with respect to work schedules, only processing activities with the sole purpose of calculating working times are covered.
 -) Regarding recovery of debt: the Board recommends the exclusion from this item of evaluation and scoring as well as exclusion of debts acquired from a third party , and further to restrict the item to debts owed in the context of a business to consumer relationship.

¹ This view is strictly tied to the present list and does not apply necessarily to similar items in the lists submitted by other Supervisory Authorities.

- J Regarding the significance of items listed: the Board encourages the French Supervisory Authority to clarify that its list is without prejudice to any other obligation stipulated by the GDPR.

4 FINAL REMARKS

21. This opinion is addressed to the Commission Nationale de l'Informatique et des Libertés (French Supervisory Authority) and will be made public pursuant to Article 64(5)(b) GDPR.
22. The French Supervisory Authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



**Opinion 14/2019 on the draft Standard Contractual Clauses
submitted by the DK SA (Article 28(8) GDPR)**

Adopted on 9 July 2019

1 CONTENTS

2	Summary of the Facts	4
3	Assessment	5
3.1	General reasoning of the Board regarding the set of standard contractual clauses	5
3.2	Analysis of the draft standard contractual clauses	5
3.2.1	General remark on the whole SCCs	5
3.2.2	Data Processing Preamble (Clause 2 of the SCCs)	6
3.2.3	The rights and obligations of the data controller (Clause 3 of the SCCs)	6
3.2.4	The data processor acts according to instructions (Clause 4 of the SCCs)	7
3.2.5	Confidentiality (Clause 5 of the SCCs)	7
3.2.6	Security of processing (Clause 6 of the SCCs)	8
3.2.7	Use of Sub-Processors (Clause 7 of the SCCs)	8
3.2.8	Transfer of data to third countries or international organisations (Clause 8 of the SCCs)	
	10	
3.2.9	Assistance to the data controller (Clause 9 of the SCCs)	11
3.2.10	Notification of personal data breach (Clause 10 of the SCCs)	13
3.2.11	Erasure and return of data (Clause 11 of the SCCs)	13
3.2.12	Inspection and audit (Clause 12 of the SCCs)	14
3.2.13	The parties' agreement on other terms (Clause 13 of the SCCs)	15
3.2.14	Commencement and termination (Clause 14 of the SCCs)	15
3.2.15	Appendix A	15
4	Conclusions	15
5	Final Remarks	15

The European Data Protection Board

Having regard to Article 28(8), Article 63 and Article 64(1)(d), (3) - (8) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the Board) is to ensure the consistent application of the GDPR throughout the European Economic Area. To this effect, it follows from Article 64(1)(d) GDPR that the Board shall issue an opinion where a supervisory authority (SA) aims to determine standard contractual clauses (SCCs) pursuant to Article 28(8) GDPR. The aim of this opinion is therefore to contribute to a harmonised approach concerning cross border processing or processing which can affect the free flow of personal data or natural person across the European Economic Area and the consistent implementation of the GDPR's specific provisions.

(2) In the context of the relationship between a data controller and a data processor, or data processors, for the processing of personal data, the GDPR establishes, in its Article 28, a set of provisions with respect to the setting up a specific contract between the parties involved and mandatory provisions that should be incorporated in it.

(3) According to Article 28(3) GDPR, the processing by a data processor *shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller*, setting out a set of specific aspects to regulate the contractual relationship between the parties. These include the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects, among others.

(4) Under Article 28(6) GDPR, without prejudice to an individual contract between the data controller and the data processor, the contract or the other legal act referred in paragraphs (3) and (4) of Article 28 GDPR may be based, wholly or in part on standard contractual clauses. These standard contractual clauses are to be adopted for those matters referred to in paragraphs (3) and (4).

(5) Furthermore, Article 28(8) GDPR determines that a SA may adopt a set of standard contractual clauses in accordance with the consistency mechanism referred to in Article 63. That is to mean that SAs are required to cooperate with other members of the Board and, where relevant, with the European Commission through the consistency mechanism. SAs are required, pursuant to Article 64(1)(d) to communicate to the Board any draft decision aiming to determine standard contractual clauses pursuant to Article 28(8). In this context, the Board is required to issue an opinion on the matter, pursuant to Article 64(3), where it has not already done so.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

(6) Adopted standard contractual clauses constitute a set of guarantees to be used as is, as they are intended to protect data subjects and mitigate specific risks associated with the fundamental principles of data protection.

HAS ADOPTED THE OPINION:

2 SUMMARY OF THE FACTS

1. The competent supervisory authority of Denmark has submitted its draft standard contractual clauses (hereafter SCCs) to the Board via the IMI system requesting an opinion from the Board pursuant to Article 64(1)(d) for a consistent approach at Union level. The decision on the completeness of the file was taken on the 4th of April 2019. The Board Secretariat circulated the file to all members on behalf of the Chair on the 4th of April.
2. The Board has received the draft SCCs from the Danish SA² along with a letter explaining the structure of the standard contractual clauses. These two documents were provided by the Danish SA in an English version. The Board hereby gives its opinion on the English version of the document although the Board notes that the SCCs is also available in Danish on the website of the Danish SA. The Danish SA shall take utmost account of the opinion of the Board.
3. In compliance with Article 10(2) of the Board Rules of Procedure³, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks (until the 9th of July 2019).

² “Data Processing agreement” is the term used by the Danish SA in the document provided to the Board to refer to Standard Contractual Clauses.

³ Version 2, as last modified and adopted on 23 November 2018.

3 ASSESSMENT

3.1 General reasoning of the Board regarding the set of standard contractual clauses

4. Any set of standard contractual clauses submitted to the Board must further specify the provisions foreseen in Article 28 GDPR. The opinion of the Board aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented draft clauses that could serve as standard contractual clauses in compliance with Article 28(8) GDPR.
5. The Board notes that the document presented to the Board is a draft SCCs containing two parts:
 - 1) a general part containing general provisions to be used as is; and
 - 2) a specific part that has to be completed by the parties with regard to the specific processing which the contract seeks to govern.
6. In addition, the Danish SA explains, in its letter, that the clauses of the SCCs which are in bold are mandatory and constitute the minimum requirements of a contract under Article 28 GDPR. The remaining clauses, although advisable to include in a SCCs, are voluntary and may be included in the SCCs at the discretion of the parties.
7. The Board is of the opinion that clauses which merely restate the provisions of Article 28(3) and (4) are inadequate to constitute standard contractual clauses. The Board has therefore decided to analyse the document in its entirety, including the appendices. In the opinion of the Board, a contract under Article 28 GDPR should further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled. It is in this light that the SCCs submitted to the Board for opinion is analysed.
8. When this opinion remains silent on one or more clauses of the SCCs submitted by the Danish SA, it means that the Board is not asking the Danish SA to take further action with regards to this specific clause. Clauses 6.4, 9.3 and 14.3 of the Danish SCCs are not required by article 28 and are related to commercial aspects and the Board therefore does not see these clauses as being part of the SCCs. It is up to the Parties whether, and how, to enter into agreement.

3.2 Analysis of the draft standard contractual clauses

3.2.1 General remark on the whole SCCs

9. The Board is of the opinion that if the SCCs only contained the sections in bold, it would not be sufficient as SCCs, since some of the non-bold sections relate to mandatory provisions under Article 28(3) GDPR. Therefore, the Board recommends that the Danish SA avoid this distinction by clearly stating, either in the clauses or in a separate document instructing on the use of these clauses, that all clauses of the SCCs together with the appendices should be included in the SCCs concluded by the parties.
10. In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority do not prevent the parties from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the adopted standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Furthermore, where the standard data protection clauses are modified, the parties will no longer be deemed to have implemented adopted standard contractual clauses.

11. The Board notes that the wording of several clauses of the SCCs are not in line with the relevant provisions of the GDPR. The Board has indicated this in its opinion below and recommends that the Danish SA align the wording of those clauses with the relevant provisions of the GDPR.

3.2.2 Data Processing Preamble (Clause 2 of the SCCs)

12. Regarding **clause 2.3** of the SCCs, the Board is of the opinion that the relationship between the data processing agreement and the “master agreement” could be more flexible. There may be cases where the standard contractual clauses are a distinct document part of the master agreement and as such, there is no need for distinct SCCs. There may also be situations where the data processing governed by the SCCs is not part of a master agreement. The Board therefore encourages the Danish SA to redraft this clause to reflect this flexibility. This specific change needs to be implemented in each occasion where the SCCs refers to the master agreement.
13. Regarding **clause 2.4** of the SCCs, first sentence, the Board is of the opinion that in some situations, the data processing agreement might be terminated before the “main agreement”. The Board recommends that the Danish SA adds, at the end of the first sentence, that the agreement *“cannot, in principle, be terminated separately, except where the data processing ends before the termination of the master agreement, or where other conditions for separate termination of the standard contractual clauses, as specified under its termination clauses, are met (see also recommendation on clause 14.4 below)”*.

3.2.3 The rights and obligations of the data controller (Clause 3 of the SCCs)

14. Regarding **clause 3.1** of the SCCs, the Board is of the opinion that the wording *“shall be responsible to the outside world”* is misleading. Indeed, it could be understood as placing obligations towards data subjects or other stakeholders solely on the data controller. The Board is of the opinion that this clause would be clearer if a reference to Article 24 GDPR and its accountability principle is made. The Board subsequently recommends that the Danish SA adds such a reference.
15. Further, regarding the clause 3.1, it would be better to refer, in general, to the applicable legislation in data protection matter, where relevant, instead of to a specific act. The Board recommends that the Danish SA amend the reference to the Data Protection Act. Finally, the Board suggests replacing the words “in the framework of” by “in compliance with”.

Therefore the Board would suggest the following wording as an example:

“1. The Data Controller is responsible for ensuring that the processing of personal data takes place in compliance with the General Data Protection Regulation (see Article 24 GDPR), the applicable EU or Member States data protection provisions () and this standard contractual clauses.”

16. Regarding **clause 3.2** of the SCCS, the Board is of the opinion that this clause is unclear, since the data controller has already defined the purposes and means of the processing activity subject to the SCCs. The Board recommends the Danish SA to modify this clause as follows:
 17. *“The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data”.*
 18. Regarding **clause 3.3** of the SCCs, the Board is of the opinion that its meaning is unclear. The Board assumes that the idea behind this clause is to make sure that the processing activities for which the data controller wishes to engage a data processor have a legal basis. If it is the case, the Board recommends that the Danish SA clarifies the clause accordingly.

Finally, the Board notes that in clause 3.1 of the SCCs the wording “processing of personal data” is used. In clause 3.3 of the SCCs, the word “processing” is used. The Board recommends that the Danish SA use the same terminology in order to avoid confusion.

As an example, the Board would therefore suggest the following wording:

“3. The data controller shall be responsible, among others, for ensuring that the processing of personal data which the data processor is instructed to perform has a legal basis.”

3.2.4 The data processor acts according to instructions (Clause 4 of the SCCs)

19. Regarding **clause 4.1** of the SCCs, the Board is of the opinion that a reference should be made to appendices A and C as they further specify the data controller’s instructions. The Board is of the opinion that additional instructions can be given by the data controller throughout the duration of the contract but such instructions shall always be documented.

Further, the Board notes that this clause is inspired by Article 28(3)(a) GDPR. The Board would therefore encourage the Danish SA to use the same wording as in the GDPR.

20. Regarding **clause 4.2** of the SCCs, the Board is of the opinion that in case of unlawful instructions, parties should foresee consequences and provide solutions.

3.2.5 Confidentiality (Clause 5 of the SCCs)

21. The Board understands clause 5 of the SCCs as the specification of Article 28(3)(b) GDPR which states that *“the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality”*.

22. Regarding **clause 5.1** of the SCCs, the word “currently” is understood by the Board as the necessity to keep the status of “authorised persons” under review. Further, it is unclear to the Board who is giving the authorisation to those persons in particular since access to personal data has to be provided on a “need-to-know” basis.

23. Regarding **clause 5.2** of the SCCs, the Board is of the opinion that this clause relates to the principle of the access to the personal data on a “need-to-know” basis. The Board is of the opinion that clauses 5.1 and 5.2 of the SCCs can be combined as follows:

“It is the responsibility of the data processor to grant access to persons under its authority to the personal data being processed on behalf of the data controller only on a need to know basis and who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The list of persons to whom access has been granted needs to be kept under periodic review. On the basis of the said review, access to personal data can be withdrawn and in this case, personal data cannot be accessible anymore to those persons.”

24. Regarding **clause 5.3** of the SCCs, the Board is of the opinion that it is covered by the suggested wording above and clause 5.3 can therefore be deleted.

25. Regarding **clause 5.4** of the SCCs, the Board recommends that the Danish SA delete the wording “*be able to*” since the data processor has to demonstrate compliance with the confidentiality requirements. Further, the Board encourages the Danish SA to adopt a broader wording when referencing to “*employees*” as there may be other persons than employees processing personal data

under the authority of the processor. Wording such as “*person under the authority of the processor*” or “*persons employed directly or indirectly by*” would be more appropriate.

3.2.6 Security of processing (Clause 6 of the SCCs)

26. Regarding **clause 6.1** of the SCCs, the Board recommends that the Danish SA replace the words “*with consideration for the current level*” in the beginning of the sentence by the words “*taking into account the state of the art*”, which is the wording of Article 32(1) GDPR. This specific wording is used in the GDPR to make sure that the level of security applied to the processing of personal data is always in line with the latest technological evolutions. The wording suggested by the Danish SA makes reference to a current level which will not be the state of the art in 2 years.
27. Regarding **clause 6.2** of the SCCs, the Board understands that this provision relates to Article 28(3)(c) of the GDPR and that clause 9.2 relates to Article 28(3)(f) of the GDPR. However, the distinction between the two clauses and the different tasks of the data processor is not very clear. The Board recalls that Article 28(3)(f) GDPR states that the data processor assists the data controller in ensuring compliance with the obligations under Articles 32 to 36 GDPR taking into account the nature of processing and the information available to the data processor.

The Board is of the opinion that the “risk assessment” referred to in the first sentence of clause 6.2 has to be performed on the processing activities, which the data controller will entrust to the data processor. The data controller should therefore provide the data processor with all the information necessary so that the data processor can comply with Article 28(3)(c) and (f) of the GDPR. The Board would like to emphasize that this does not exempt the data controller from the responsibility to be in compliance with its own obligations under Article 25, 32 or 35-36 GDPR.

In addition, the end of the first sentence of clause 6.2 needs to be redrafted in order to be more in line with clause 9.2 and appendix C2 as it is not clear for the Board how the wording “*thereafter implement measures to counter the identified risk*” in clause 6.2 is related to clause 9.2 and appendix C2. The Board has noticed that clause 9.2.a and appendix C2 address the topic of risk assessment but not in the same way as clause 6.2. Under clause 6.2, the risk assessment is to be performed by the data processor, whereas under clause 9.2 and appendix C2, the risk assessment is to be performed by the data controller. Appendix C2 further sets out that the data processor shall implement measures that have been agreed with the data controller.

Regarding appendix C2, the Board is of the opinion that the wording “*The level of security shall reflect*” could be changed into “*The level of security shall take into account*”. Regarding the elements to be taken into account, Articles 32(1) and 32(2) GDPR mentions the nature, scope, context and purposes of the processing activity as well as the risk for the rights and freedoms of natural persons. These could be elements to mention in order to clarify what is expected by “*Describe elements that are essentials to the level of security*”.

Therefore, the Board recommends that the Danish SA clarifies and aligns clauses 6.2, 9.2 and Appendix C2.

3.2.7 Use of Sub-Processors (Clause 7 of the SCCs)

28. Regarding **clauses 7.2 and 7.5** of the SCCs, the Board recommends that the Danish SA replace the word “consent” by “authorisation”, as this is the wording of Article 28(2) GDPR.

Furthermore, the Board is of the opinion that it would be more practical to create options in this clause as follows:

"2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of these standard contractual clauses without the prior [Choice 1] specific authorisation of the data controller / [Choice 2] general written authorisation of the data controller."

29. Regarding **clauses 7.3 and 7.4** of the SCCs, the Board finds it important to add the fact that the list of sub-processors which are accepted by the data controller at the time of the signature of the contract should be included as an appendix to the SCCs, be it on the basis of a general authorisation or a specific one. The purpose of this list is to ensure that even in cases of a general authorization, the data controller remains informed about the list of sub-processors as well as further changes. The Board recommends that the SCC clarifies that the list of sub-processors in appendix B2 has to be provided both in cases of general and specific prior authorisation.

Further, in appendix B1 of the SCCs, there are examples of clauses that the parties can choose in-between. The Board considers that it would, however, be better to include such clauses in the SCCs itself instead of in the appendices.

Finally, as regards the general prior authorisation, the Board is of the opinion that any conditions that the data processor might set for the data controller to object to changes of sub-processor(s) must allow the data controller to, in practice, exercise its freedom of choice and enable the data controller to remain in control over the personal data. This implies also that the data controller should have sufficient time to object to such a change.

The Board recommends that the Danish SA redraft clause 7.3 to create options within the clause that can be chosen by the parties within the SCCs and to incorporate the content of clauses 7.4 and 7.5 within 7.3.

Clause 7.3 could be drafted as follow:

"3. In case of general written authorisation, the data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors in at least [specify time period], and thereby giving the data controller the opportunity to object to such changes prior to the engagement of any sub-processor. Longer time periods of prior notice for specific sub-processing services can be provided in the Appendix B. The list of sub-processors already accepted by the data controller can be found in appendix B."

In case of specific prior authorisation, the data processor shall engage sub-processor solely with the prior authorisation of the data controller. The data processor shall submit the request for specific authorisation at least [specify time period] prior to the engagement of any sub-processor. The list of sub-processors already accepted by the data controller can be found in appendix B."

As the option is created in the draft SCCs itself, appendix B1 can be deleted. In addition, the Board recommends that the Danish SA adds a possibility to have a longer period of prior notice in appendix B.

30. Regarding **clause 7.6** of the SCCs, the Board understands this clause as a reference to Article 28(4) GDPR. As previously mentioned, it would be better to refer to the exact wording of the text of the GDPR to avoid any confusion.

Regarding **clause 7.8** of the SCCs, the Board would like to underline the fact that its content is not required by Article 28 GDPR. The Board is of the opinion that the words "third party" are unclear. If

the intention is to create a “third party beneficiary right” for the data controller within the contract between the data processor and the sub-processor, this should be specified.

As such, the Board sees an added value in having such a clause as part of a standard contractual clauses. Indeed, it preserves the rights of the data controller, including liability. For this reason, the Board encourages the Danish SA to make it clearer that the intention is to create a third beneficiary right for the data controller. This would imply for instance that the sub-processor would accept to be liable to the data controller in case of the initial data processor is bankrupt or the possibility for the controller to directly order the sub-processor to return the data.

31. Regarding **clause 7.9** of the SCCs, the Board is of the opinion that it is important to make a reference to the rights of the data subject. This reference can be made as follows: *“This does not affect the rights of the data subjects under the GDPR - in particular those foreseen in Articles 79 and 82 GDPR - against the data controller and the data processor, including the sub-processor.”*

3.2.8 Transfer of data to third countries or international organisations (Clause 8 of the SCCs)

32. Regarding the title of the clause, the Board is of the opinion that it should be clarified that the words “third countries” refers to countries outside of the EEA and not outside of Denmark. The Board encourages the Danish SA to clarify this.
33. The Board is of the opinion that section 8 should clarify that the data controller has to decide whether a transfer is allowed under the contract or if it should be prohibited. The Board recommends to the Danish SA that this is made clear in the standard contractual clauses and encourages it to specify this in appendix C5.
34. Regarding **clause 8.1** of the SCCs, the Board notes that the Danish SA has added parentheses after the word “transfer” as following “(assignment, disclosure and internal use)”. The Board wonders whether this aims at giving a definition of the word “transfer”. If this is the intention, the Board is of the opinion that as there is no such definition of the notion of transfer in the GDPR, it is better to delete these terms in parentheses.

Finally, the Board recommends that the Danish SA start its clause 8.1 by adding *“In compliance with Chapter V GDPR ...”* Indeed, the Board recalls that for any transfer outside of the EU, all provisions of Chapter V GDPR need to be complied with. It should be clarified under clause 8 that these SCCs cannot be understood as SCCs fulfilling the requirements of Art. 46 GDPR and therefore cannot be used as a tool to carry out international transfers within the meaning of Chapter V of the GDPR. This could be in addition reflected in the title of clause 8, which otherwise may give the impression that transfers can be carried out on the basis of these SCCs.

35. Regarding **clause 8.2** of the SCCs, the Board has several remarks.

First, in the beginning of the sentence, the Board encourages the Danish SA to add the word “documented” before “instructions” to ensure legal certainty and alignment with Article 28(3)(a) GDPR and to change the word “*approval*” to “*authorisation*” in line with the terms used under Article 28 GDPR. The beginning of the sentence should be *“Without the documented instructions or authorisation of the data controller”*.

Second, on clause 8.2.a, the word “*disclose*” might create confusion with the notion of transfer. In addition, personal data can be transferred to a data controller (as already mentioned in the clause) but also to a data processor in a third country. The Board recommends that the Danish SA drafts clause

8.2.a as follows: "*transfer personal data to a data controller or a data processor in a third country or in an international organisation*".

Third, on clause 8.2.b, the word "assign" might also create confusion with the notion of transfer. The Board recommends that Danish SA replace the word "assign" by the word "transfer".

Finally, on clause 8.2.c, it is unclear to the Board what the meaning of the word "divisions" is. The Board encourages the Danish SA to replace clause 8.2.c by the following sentence: "*have the data processed by the Data Processor outside the EEA*".

36. Regarding **clause 8.3** of the SCCs, the Board understands that it is a way to have the instructions of the data controller documented in the appendix C5. As already stated in the beginning of its opinion, the Board sees the appendices as mandatory. However, the Board is of the opinion that mentioning the choice of the tool for transfer could have a benefit, in addition to the instructions as it contributes demonstrating compliance of the parties with Chapter V of the GDPR. The Board encourages the Danish SA to amend clause 8.3 as follow:
37. "*The data controller's instructions regarding transfers of personal data to a third country including, if applicable, the transfer tool on which they are based, shall be set out in appendix C5 of these standard contractual clauses. The same procedure shall be applied for the approval of transfers of personal data to a third country.*"

3.2.9 Assistance to the data controller (Clause 9 of the SCCs)

38. **Clause 9.1** of the SCCs reflects the content of Article 28(3)(e) of the GDPR. The obligation of the data processor under this clause is to assist the data controller to respond to requests for exercising data subject's rights. The assistance can take various forms. The Board is of the opinion that the SCCs needs to give details on the manner in which the processor is required to provide assistance and not only the list of possible rights to be exercised.

Notably, the SCCs should set out the steps to be taken by the data processor in case the latter directly receives a request from a data subject relating to the exercise of his/her rights. For example, it has to be clear in the agreement in such a case as to whether the data processor is not allowed to have any contact with the data subjects, and how the processor needs to inform the controller when it comes to data subjects' rights (e.g. forwarding the request to the controller within a specified timeframe or other appropriate measures). In this case, the assistance is provided only through an exchange of information between the data controller and the data processor. Another scenario could be that the data controller instructs the data processor to answer to data subject's requests according to instructions given. Another option could be that the data processor would make the technical implementations instructed by the data controller with respect to data subject rights. The Board recommends that the Danish SA reflect on the possibility to include the following sentence under clause 9.1 of the SCCs:

"The parties shall define in appendix C the appropriate technical and organisational measures with which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in clauses 9.1 and 9.2 of the standard contractual clauses."

A new point in appendix C needs to be created in order to have the technical and organisational measures specified.

Further, on clause 9.1.a and 9.1.b the Board recommends that the Danish SA use the words "*right to be informed*" instead of the word "*notification*", as follow: "*Right to be informed when collecting personal data from the data subject*" - "*Right to be informed when personal data have not been obtained from the data subject*".

Regarding clause 9.1.j, the Board would prefer to have the exact wording of the GDPR. The Board therefore encourages the Danish SA to redraft it as follow "*the right not to be subject to a decision solely based on automated processing, including profiling*".

39. **Clause 9.2** of the SCCs reflects the content of Article 28(3)(f) of the GDPR. Hence the Board recommends replacing "*data made available*" by "*information available*". The obligation of the data processor under this clause is to assist the data controller for the fulfilment of the legal duties relating to the security, the data protection impact assessment and prior consultation of SAs. Here again, the Board is of the opinion that the SCCs needs to give details on the manner in which the data processor is required to provide assistance to the data controller.

As already stated in paragraph 27 of this opinion, the Danish SA should clarify the relationship between clause 9.2 and clause 6 on security of the processing. The Board understands the relationship between those two clauses as referring to Article 28(3)(c) of the GDPR for clause 6 and to Article 28(3)(f) for clause 9.2. Indeed, clause 9.2.a and to a certain extent clause 9.2.b are obligations that need to be fulfilled in all cases by the data processor subject to the GDPR. This follows from Article 32(1) and Article 33(2) GDPR. For clause 9.2.a to be kept, some further alignments with Article 32(1) GDPR would be required. The Board recommends to the Danish SA to make clear that the risk would be the risk "for the rights and freedoms of natural persons". Furthermore, not only is the nature of the processing to be taken into account, but also the state of the art, the costs of implementation, the scope, the context and the purposes of the processing. The Board understands that the parties should specify in Appendix C2 the minimum level of security and measures to be implemented by the data processor. The Board considers it important that details on assistance to the data controller as regards security of the processing be included in the instructions under appendix C2.

The Board has provided a drafting suggestion covering clauses 9.1 and 9.2 above.

On clause 9.2.b, the Board is of the opinion that any reference to a specific national supervisory authority in a model contract should be avoided. In addition, the words "*report*" should be replaced by "*notify*" and "*discovering*" should be replaced by "*after becoming aware*" to be in line with Article 33(2) GDPR.

Clause 9.2.b could be drafted as follow: "*b. its obligation, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, to report personal data breaches to the competent supervisory authority, [PLEASE INDICATE the competent SA], without undue delay and where feasible, no later than 72 hours after having become aware of such breach*".

On clause 9.2.e, here again, the Board is of the opinion that the reference to the Danish SA should be removed. Clause 9.2.e could be drafted as follow: "*e. the obligation to consult the competent supervisory authority, [PLEASE INDICATE the competent SA], prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk*".

The Board considers important to have this clause further detailed in appendix C or D to ensure that the parties make arrangements on the manner this assistance will be provided in practice.

3.2.10 Notification of personal data breach (Clause 10 of the SCCs)

40. Regarding **clause 10.1** of the SCCs, the Board, as already stated, favours the wording of the GDPR in order to avoid any confusion. In this clause, the word “discovery” should be changed into “after having become aware”. In addition, the Board encourages the Danish SA to add the word “any” before personal data breach in order to make clear that it is not up to the data processor to assess whether or not the data breach has to be notified to the competent SA. This is the data controller’s responsibility⁴.

The sentence could be changed as follow: “*1. In case of any personal data breach, the data processor or sub-processor shall, without undue delay after having become aware of it, notify the data controller.*”

The Board recommends deleting “*at the data processor’s facilities or a sub-processor’s facilities*” which would limit the notification obligation to cases where the breach occurs in these facilities, whereas such limitation does not stem from the GDPR.

Regarding the second part of clause 10.1, the Board is of the opinion that it can be completed as follows:

“The data processor’s notification to the data controller shall, if possible, take place with-in [number of hours] after the data processor has become aware of the breach in order to enable the data controller to comply with his obligation to report personal data breaches already mentioned in clause 9.2.b. ”

41. Regarding **clause 10.2** of the SCCs, the Board is of the opinion that the words “*taking into account the nature of the processing and information available*” could be further specified in appendix D in order to be more concrete and tailor-made. The following wording could be added in a new paragraph at the end of clause 10.2:

“The parties shall define in appendix D the elements to be provided by the data processor to assist the data controller in the reporting of a breach to the supervisory authority.”

In addition, in the beginning of the second sentence of clause 10.2, the draft SCCs states “*This may mean - on the basis of the information available to the Processor - (...)*”. The Board is of the opinion that - for the sake of legal certainty - it is better to avoid this kind of formulation. The Board encourages the Danish SA to amend this wording by deleting the word “may”.

3.2.11 Erasure and return of data (Clause 11 of the SCCs)

42. Regarding **clause 11** of the SCCs, the Board is of the opinion that it would be more practical to create a real option in this clause. The Board encourages the Danish SA to amend this clause in order to create two concrete options to be chosen by the Data Controller.

The clause could be drafted as follows:

⁴ See Guidelines on data breach notification (p. 13) “It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller.”

"On termination of the processing services, the data processor shall be under obligation [Option 1] to delete all personal data processed on behalf of the data controller [Option 2] to return all the personal data to the Data Controller and to erase existing copies.

[Optional] The following EU or Member states law applicable to the processor requires storage of the personal data after the termination of the processing services: The processor commits to exclusively process the data for the purposes provided by this law and under the strict applicable conditions."

More information could be provided in the appendix C3, including the possibility for the data controller to modify the option chosen at the signature of the contract. This, as a consequence, affects the content of appendix C3. The Board encourages the Danish SA to better distinguish the storage period from the erasure procedures under appendix C3 and to reflect the possibility for the data controller to change the choice made.

Finally, the Board is of the opinion that the words "processing services" need to be specified for instance by "after the end of the provision of services relating to processing". This can be done in the appendix D.

[**3.2.12 Inspection and audit \(Clause 12 of the SCCs\)**](#)

43. **Clause 12.1** of the SCCs reflects the content of Article 28(3)(h) of the GDPR. The Board recommends to use the same terminology of paragraph 1 "audits, including inspections" within paragraphs 2 and 3 which only refer to inspection.
44. Regarding **clause 12.3** of the SCCs, the Board understands it as covering audit and inspections towards the sub-processor. In accordance with Article 28(4) of the GDPR, the same obligations as set out in the contract or another legal act between the controller and the processor shall be imposed on the sub-processor. This includes the obligation under Art. 28(3)(h) to allow for and contribute to audits by the data controller or another auditor mandated by the data controller. The drafting of clause 12.3 seems to limit this right of the data controller vis-a-vis the sub-processor ("if applicable" and "performed through the Data processor"). The Board recommends that the Danish SA redrafts clause 12.3 in order to be in full compliance with the GDPR. This can be done by merging clauses 12.2 and 12.3 as follows: *"Procedures applicable to the data controller's audits, including inspections of the data processor and the data sub-processor are specified in appendices C6 and C7 to these standard contractual clauses."*
45. Regarding appendices C6 and C7, the Board recommends the Danish SA to change the following sentence *"The inspection report shall without delay be submitted to the Data Controller for information purposes"* to make it clear that the controller is be able to contest the scope, methodology and the results of the inspection. The controller should also be able to request measures to be taken following the results of the inspection.
46. In addition, the reference is appendix C6 to "*Data Processor's facilities*" and C7 to "*Sub-Processor's facilities*" need to be broaden. Indeed, rights of the data controller in the framework of inspections and/or audit should not be limited to the facilities of the processor or sub-processors. The data controller should have access to the places where the processing is being carried out. This includes physical facilities as well as systems used for and related to the processing.

3.2.13 The parties' agreement on other terms (Clause 13 of the SCCs)

47. Regarding **clause 13** of the SCCs, the Board recommends that the Danish SA bear in mind that if a paragraph specifying liability, governing law, jurisdiction or other terms is included, it cannot lead to any contradiction with the relevant provisions of the GDPR or undermine the level of protection offered by the GDPR or the contract.

3.2.14 Commencement and termination (Clause 14 of the SCCs)

48. Regarding **clause 14.4** of the SCCs, the Board is of the opinion that a specific provision on the termination of the contract might also be relevant for the SCCs. As the position of the Board is that the relationship between the data processing agreement and the master agreement should be more flexible, the Board recommends that the Danish SA includes a provision on the termination within the SCCs.
49. Regarding **clause 14.5** of the SCCs, the Board is of the opinion that this clause might be in contradiction with clauses 2.4 or 14.4. The Board recommends that the Danish SA clarifies the relationship between those three clauses.

3.2.15 Appendix A

50. Appendix A aims at giving details about the processing activities undertaken by the data processor on behalf of the data controller. To this end, the Board recommends that the purpose and the nature of the processing are described, as well as the type of personal data processed, the categories of data subjects concerned and the duration of the processing. This description should be made in the most detailed possible manner, and, in any circumstance, the types of personal data must be specified further than merely "personal data as defined in article 4(1)" or stating which category (Article 6, 9 or 10) of personal data is subject to processing. The Board is of the opinion that it should be clear that in case of several processing activities, these elements have to be completed for each of them. In addition, the Board is not convinced by the two first examples, as it is difficult to distinguish the purpose to the nature of the processing.

4 CONCLUSIONS

51. The Board very much welcomes the Danish initiative to submit their draft SCCs for an opinion which aim at contributing to an harmonized implementation of the GDPR.
52. The Board is of the opinion that the draft SCCs of the Danish Supervisory Authority submitted for an opinion need further adjustments in order to be considered as standard contractual clauses. The Board made several recommendations in its opinion here above. If all recommendations are implemented, the Danish SA will be able to use this draft agreement as Standard Contractual Clauses pursuant to article 28.8 GDPR without any need for a subsequent adoption from the EU Commission.

5 FINAL REMARKS

53. This opinion is addressed to Datatilsynet (the Danish Supervisory Authority) and will be made public pursuant to Article 64 (5b) GDPR.

54. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft SCCs. Within the same period, it shall provide the amended draft SCCs⁵ or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁵ The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

Opinion of the Board (Art. 64)



Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc.

Adopted on 8 October 2019

Table of contents

1	Summary of the facts	4
2	Assessment.....	4
3	Conclusions / recommendations.....	5
4	Final remarks	5

The European Data Protection Board

Having regard to Article 63, Article 64 (1) (f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25th May 2018 as last modified and adopted on 10 September 2019,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. To this effect, it follows from article 64(1)(f) GDPR that the Board shall issue an opinion where a supervisory authority (SA) aims to approve binding corporate rules (BCRs) within the meaning of article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under the Directive 95/46/EC the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of article 47 GDPR and, in addition, conferred to the EDPB the task to issue an opinion on the competent supervisory authority’s (BCR Lead) draft decision aiming to approve BCRs. This task of EDPB aims to ensure the consistent application of the GDPR, including by the supervisory authorities, controllers and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (article 47(2) GDPR). The BCRs are subject to approval from the competent supervisory authority (“competent SA”), in accordance with the consistency mechanism set out in article 63 and 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party¹, endorsed by the EDPB.

¹ The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) WP256 rev.01 of the Article 29 Working Party,² as endorsed by the EDPB, provides for the required elements for BCRs for controllers, including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance to the supervisory authorities' national laws. The EDPB is subject to Regulation 1049/2001 pursuant to article 76(2) GDPR.

(5) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2), each application should be addressed individually and is without prejudice to the assessment of any other Binding Corporate Rules. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake and the policies and procedures that they have in place to protect personal data.³

(6) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in the WP263 rev.01, the draft Controller BCRs of Equinix Inc. were reviewed by the Information Commissioner of the United Kingdom (UK Supervisory Authority) as the BCRs Lead SA.
2. The Information Commissioner of the United Kingdom has submitted her draft decision regarding the BCRs of Equinix Inc., requesting an opinion of the Board pursuant to article 64(1)(f) GDPR on 25/09/2019. The decision on the completeness of the file was taken on 25/09/2019.

2 ASSESSMENT

3. The draft BCRs of Equinix Inc., contained in the Global Privacy Policy and its Appendices, cover personal data transferred from entities of Equinix Inc. in the EEA to entities of the group outside the EEA and processed by those entities outside the EEA. The related categories of data subjects include employees and business contacts, i.e. suppliers and vendors.

² Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018 , WP 256 rev.01.

³ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

4. The company may apply different standards for the processing and transfer of personal data that do not fall within this draft BCRs while these standards may be included in the same document, i.e. the Global Privacy Policy.
5. The Equinix BCRs have been scrutinised according to the procedures set up by the EDPB. The SAs assembled under the EDPB have concluded that the Equinix BCRs contains all elements required under article 47 GDPR and WP256 rev01, in concordance with the draft decision of the Information Commissioner of the United Kingdom submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns which need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that Equinix Inc. will undertake by signing the Equinix Intra-Company Agreement on Binding Corporate Rules, the EDPB considers that the draft Decision of the Information Commissioner of the United Kingdom upon the Binding Corporate Rules of Equinix group may be adopted as it is, since those Rules ensure appropriate safeguards to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined when personal data will be transferred to and processed by the Group Members based in third countries. Finally, the EDPB also recalls the provisions contained within article 47(2)(k) GDPR and WP 256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs Group Members

4 FINAL REMARKS

7. This opinion is addressed to the Information Commissioner of the United Kingdom and will be made public pursuant to article 64(5)(b) GDPR.
8. In accordance with article 64(7) and (8) GDPR, the Information Commissioner shall communicate her response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to article 70(1)(y) GDPR, the Information Commissioner shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 1/2020 on the Spanish data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 28 January 2020

Table of contents

1	Summary of the facts	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the ES accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	6
2.2.3	CONFLICT OF INTEREST	7
2.2.4	EXPERTISE.....	8
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	8
2.2.6	TRANSPARENT COMPLAINT HANDLING.....	9
2.2.7	COMMUNICATING WITH THE AEPD.....	10
2.2.8	CODE REVIEW MECHANISMS.....	10
2.2.9	LEGAL STATUS	10
3	CONCLUSIONS / RECOMMENDATIONS.....	11
4	FINAL REMARKS	12

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018, as last modified and adopted on 10 September 2019

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, to provide written guidance explaining the accreditation requirements; and, finally, requesting them to adopt these requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term ‘accreditation’. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

their proposed monitoring body meets the requirements set out in article 41 (2) to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Spanish Supervisory Authority (hereinafter "ES SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 25 October 2019.
2. In compliance with article 10 (2) of the Board Rules of Procedure,² due to the complexity of the matter at hand, the Board decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements
3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation

² Version 3, as last modified and adopted on 10 September 2019.

section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.

4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.
5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the ES SA to take further action.
8. This opinion does not reflect upon items submitted by the ES SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the ES accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The wording in the ES SA's accreditation requirements is not in line with the terminology used in the Guidelines. For the sake of consistency and clarity, the EDPB encourages the ES SA to use the Guidelines terminology in the draft accreditation requirements. Examples include: “Accreditation requirements” instead of “Accreditation criteria” in the title, “code owners” instead of “code sponsor or code promoter”, “code members” instead of “supervised bodies”, “monitoring body” instead of

“supervisory body”, “internal body” instead of “inside body”, “establishment [of the monitoring body]” instead of “seat [of the monitoring body]”. The paragraphs concerned are 1, 1.1, 1.2, 1.3, 1.4, 2, 3, 3.1, 3.2, 5.2, 5.3, 6.2, 6.3, 7.1, 8, and 8.2.

11. Whereas the Board acknowledges that reference to “should” might be due to the translation of the Spanish terms used to express obligation, the Board recommends that the ES SA amends the wording throughout the draft accreditation requirements, and replaces it with either “shall” or “must” in order to ensure the enforceability of the requirements.
12. The Board notes that there is no reference to the duration of the accreditation or accreditation withdrawal procedures. Whilst the Board accepts that these areas fall into the area of guidance supporting the accreditation requirements, the Board considers them to be important areas in terms of ensuring that the whole accreditation process is transparent. Therefore, the Board encourages the ES SA to clarify accreditation duration and withdrawal procedures in supporting guidance for the accreditation requirements.
13. Finally, the Board understands that, unless explicitly stated otherwise, the ES SA draft accreditation requirements apply to both internal and external monitoring bodies.

2.2.2 INDEPENDENCE

14. With regard to the introduction of section 1 of the draft accreditation requirements, the Board takes note of all the elements demonstrating the monitoring body’s independency and impartiality of function in relation to the code members and the profession, industry or sector to which the code applies. However, there seems to be a contradiction between the third and fourth paragraphs of this section. In the third paragraph it is stated that the monitoring body should not have *“any dependency of any kind (organisational, economic, professional or personal) on the affiliated entity”*, which seems to exclude the possibility of accrediting internal monitoring bodies on the basis of the fulfillment of this requirements. At the same time, in the last paragraph, there is mention of cases where the monitoring body is internal. Therefore, the Board recommends to the ES SA to clarify the relationship between these two paragraphs, and explain how independence can be achieved by an internal monitoring body, as well as to redraft the third paragraph so that internal monitoring bodies are suitably covered.
15. With regard to requirement 1.1, third bullet point, the Board considers that the wording *“[...] are being supervised [...] by the sponsor of the code of conduct, when the monitoring body is an inside body”* seems to weaken the separation between the code owners and the code members on the one hand, and the monitoring body on the other. Indeed, according to the Guidelines (paragraph 65, page 22), where an internal monitoring body is proposed, there should be separate staff and management, accountability and function from other areas of the code owners’ organisation. In addition, the monitoring body, even if it is an internal one, should ensure adequate impartiality and independence on the basis of a risk management approach. Consequently, the Board recommends that the ES SA deletes the sentence *“or by the sponsor of the code of conduct, when the monitoring body is an inside body”*, or otherwise clarify it, in line with the Guidelines.
16. As for the financial requirements (section 1.3 of the ES SA draft accreditation requirements), the Board acknowledges that monitoring bodies should be provided with the financial stability and resources

necessary for the effective performance of their tasks. The means by which a monitoring body receives financial support should not adversely affect the independence of its task of monitoring compliance of a code. The funding of the monitoring body and the transparency of such funding constitute a decisive element to assess the independence of the monitoring body. For this reason, the Board recommends that the ES SA deletes the phrase “where appropriate” and replaces “should” by “must be” or “have to be provided” in section 1.3 of the ES SA draft accreditation requirements.

17. Furthermore, section 1.4 of the ES SA draft accreditation requirements expressly refers to the “*cases where the monitoring body is an inside body [internal body]*”. The Board encourages the ES SA to clarify that the means of financing would not adversely affect the independence of the internal monitoring body.
18. The Board notes the requirement for the monitoring body to provide a description of resources available to it, in order to meet its liabilities as a result of its failure to perform its tasks (section 8.3 of the ES SA draft accreditation requirements). However, the Board is of the opinion that such a requirement might appear disproportionately burdensome for small and medium entities that might be discouraged from applying for accreditation. In this regard, the Board recommends that the ES SA softens the wording of this section, referring to the monitoring body’s responsibilities in a general manner.
19. Regarding the publication of the monitoring body’s report of annual activities (section 6.1), the Board recommends that, for the sake of clarity, the ES SA specifies the information that is deemed relevant for publication, as well as the level of detail of information that needs to be included in such reports.
20. The Board observes that there are no references to accountability as one of four areas in which the monitoring body shall demonstrate independence. According to the Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR, “*the monitoring body shall be able to demonstrate “accountability” for its decisions and actions in order to be considered to be independent*” (paragraph 24). In this regard, the Board recommends that the ES SA includes the obligation to demonstrate independence in relation to the accountability of the monitoring body. For example, the ES SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. This could be accomplished through such things as setting out the roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the staff about the governance structures and the procedures in place.

2.2.3 CONFLICT OF INTEREST

21. The Board takes note of all the requirements included in the ES SA accreditation requirements in order for the monitoring body to demonstrate that the exercise of its tasks and duties does not result in a conflict of interest. However, the introduction under section 2 does not provide enough clarity as to which situations may result in a conflict of interest. The Board is of the opinion that, for practical reasons, examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the

organisations adhering to the code. Therefore, the Board encourages the ES SA to add some examples, similar to the one provided in this paragraph.

2.2.4 EXPERTISE

22. Section 3 of the ES SA accreditation requirements refers to the “*promoters of the code of conduct*” and “*sponsor of the code*” (understood as code owners) and the monitoring body, who need to demonstrate that “*the persons in charge of taking decisions have the necessary knowledge in relation to data protection legislation and practice [...]*”. The Board is of the opinion that reference to the obligation of the code owners to demonstrate the expertise of the monitoring body could be misleading. Indeed, it might be appropriate in case of an internal monitoring body applying for accreditation, whereas in the case of an external monitoring body, it would be the body itself, applying for accreditation, that would need to demonstrate its expertise. Therefore, the Board encourages the ES SA to delete the phrases “*promoters of the code of conduct*” and “*sponsor of the code*” in order to refer to both internal and external monitoring bodies.
23. Furthermore, the Board encourages the ES SA to align the first paragraph of this section to the Guidelines, by including reference to the required expertise in “[...] *data protection legislation and practice in the processing activities of the sector [...]*”. Finally, the Board encourages the ES SA to clarify the third paragraph of this section by indicating that the requirement for expertise applies to the monitoring body as a whole and not to every staff member.
24. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (in section 6.4 of the Guidelines), by demonstrating “*why their proposals for monitoring are appropriate and operationally feasible*” (paragraph 41, page 17 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code’s monitoring activities effectively. Section 3.1 of the ES SA draft accreditation requirements refers to the “*means to demonstrate the necessary skill, knowledge and experience*”. A reference to the level of experience as required by the code itself is missing. The Board encourages the ES SA to add examples so that the data protection expertise, experience and knowledge required, are reflected in the Code itself.
25. Section 3.2 of the ES SA draft accreditation requirements provides only a general description of the expertise requirements. The Board encourages the ES SA to provide a detailed description of the expertise requirements and clarify whether the requirements set in paragraph 69 of the Guidelines are covered.
26. Finally, in order for these requirements to be actual requirements, rather than guidance, the Board encourages the ES SA redraft all three requirements to start with “*the monitoring body shall...*”.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

27. The Board notes that requirement 5.2 of the ES SA accreditation requirements states that the complaint handling procedure will be transparent and easily accessible to the public. The Board acknowledges that this wording is based on the Guidelines. Nonetheless, the Board is of the opinion that, for the sake of clarity, the requirements should specify the meaning of “public” and whether it also includes code members. Therefore, the Board encourages the ES SA to amend requirement 5.2 accordingly.

28. The Board observes that among the factors to consider when assessing the details of the procedures aiming at monitoring the compliance of the code members with the code of conduct (section 4.1, second bullet point of the ES SA draft accreditation requirements) the requirement refers to "*the number of members*". It is unclear, how the assessment of the ES SA could be based on this criterion, considering that the numbers of the code members might not be known when the monitoring body applies for accreditation and might change considerably after the accreditation has been granted. Among the said factors, there is also a reference to "*the number of complaints received*". Whereas the number of complaints could be relevant, the focus thereof is probably more relevant as a criterion, but it is not included. Furthermore, the Board considers that other elements, such as the focus of the complaints, might have a greater significance. In this regard, the Board encourages the ES SA to replace the term "*the number of members*" with "*expected number and size of members*" and to delete reference to the "*number*" of complaints, and keep it more general, such as "*the received complaints*".

2.2.6 TRANSPARENT COMPLAINT HANDLING

29. Regarding the complaints about code members (section 5.2 of the ES SA draft accreditation requirements), the Board acknowledges that the complaints handling process requirements should be set at a high level and reference reasonable time frames for answering complaints. In this regard, the Board notes that the ES SA draft accreditation requirements state that the complaints procedure should be resolved "*within a reasonable period of time not exceeding three (3) months*". In the event that, by the term "*resolve*", the ES SA refers to the final decision of the investigation, the Board recommends the ES SA to take a more flexible approach, by stating that the monitoring body will have to provide the complainant with progress reports or the outcome within a reasonable timeframe, such as three months. If the ES SA refers to another kind of resolve, different from the final decision of the investigation, the Board recommends the ES SA to clarify what kind of information it is referring to.
30. Furthermore, the Board takes note of the fact that the three months deadline could be extended where necessary, considering the size of the company under investigation, as well as the difficulty of the investigation.
31. The Board observes that section 5.2, fifth bullet point of the ES SA draft accreditation requirements only refers to "*penalties*". In the Board's opinion, this requirement seems to restrict the margin of manoeuvre of the monitoring body with regard to the kind of measures it can apply. In addition, those measures must be determined in the code of conduct, as per article 40(4) GDPR. The Board considers that a more comprehensive wording would include reference to remedies and corrective measures and encourages the ES SA to replace "*penalties*" with "*sanctions*". Those corrective measures must be determined in the code of conduct, as per article 40(4) GDPR. Therefore, for the sake of clarity, the Board recommends the ES SA to add a reference to the list of sanctions set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.
32. The Board observes that the ES SA decides, for the purpose of transparency of the complaints handling procedure, to require that the monitoring body publishes the decisions taken in the context of the complaint handling procedure (section 5.2). Publication of final decisions could have the same effect of an accessory sanction for the code member to which the decision is addressed. However, the Board acknowledges that general information on the actions taken by the monitoring body in case of

infringement of the code of conduct would enhance transparency. Thus, for the sake of clarity, the Board recommends that the ES SA specifies the kind of relevant information that the monitoring body is obliged to publish. For example, the monitoring body could publish, on a regular basis, statistical data with the result of the monitoring activities, such as the number of complaints received, the type of infringements and the corrective measures issued.

2.2.7 COMMUNICATING WITH THE AEPD

33. The Board observes that there is no reference to a deadline by which the monitoring body should inform the AEPD in the event of a substantial change (section 6.2 of the ES SA draft accreditation requirements). Therefore, the Board recommends that the ES SA rephrases the requirement to cover appropriate time expectations for the communication to the AEPD. For example, a substantial change shall be communicated to the ES SA “without undue delay”. Furthermore, the “*scope of accreditation*” is amongst the substantial changes that shall be reported to the SA (section 6.2, fourth bullet point). The Board considers this inclusion misleading, since the monitoring body cannot change the scope of the accreditation. Therefore, the Board recommends that the ES SA deletes reference to the scope of accreditation or, alternatively, clarify the meaning thereof.
34. The Board observes that section 6.3 of the ES SA accreditation requirements refers to the elements that communication to the AEPD should contain; the reasons for the decision as well as the criteria on which the suspension is based. For reasons of clarity, the Board recommends that reference to “exclusion” is added as well.

2.2.8 CODE REVIEW MECHANISMS

35. The Board considers that the requirements under section 7.1 appear to be too strict and might lead to excessive standards for the monitoring body, especially the third and fourth bullet points. It should be sufficient that the monitoring body shall inform the code owner and recommend that the relevant parts of the code are revised in accordance with the evaluation. In addition, this requirement should envisage the possibility that the information listed in it is not provided to the code owner, but to any other entity referred to in the code of conduct, in order to give some margin of manoeuvre to the code owners in designing the procedure for assessing the necessity of a revision of the code. In this regard, the Board encourages the ES SA to rephrase the last two bullet points, so that they appear less restrictive, as well as include information to remedy the identified shortcomings. Furthermore, the Board considers that more flexibility should be allowed, and encourages the ES SA to take into consideration that the information listed in the requirement may be not be provided to either the code owner, or to any other entity referred to in the code of conduct and add the above-mentioned reference.

2.2.9 LEGAL STATUS

36. Section 8.1 of the ES SA draft accreditation requirements includes reference to the legal personality of the monitoring body; however, an internal monitoring body is unlikely to have a legal personality. This

requirement would in fact impede an internal monitoring body from applying for accreditation. Consequently, the Board recommends to the ES SA to delete reference to the “*legal personality*” in order to clarify that internal monitoring bodies are not excluded.

37. Finally, the Board notes that the ES SA’s requirements or explanatory notes do not reference subcontracting, leaving this area open for monitoring bodies applying for accreditation to decide upon. The Board recommends that ES SA clarifies whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the explanatory notes or ordinance accordingly. If ES SA indicates that subcontracting is allowed, the Board recommends that the ES SA indicates, in the requirements, that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

3 CONCLUSIONS / RECOMMENDATIONS

38. The draft accreditation requirements of the Spanish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
39. Regarding *general remarks* the Board recommends that the ES SA:
1. replaces “*should*” with “*shall*” or “*must*” throughout the text, in order to ensure the enforceability of the requirements.
40. Regarding *independence* the Board recommends that the ES SA:
1. clarifies and explains how independence can be achieved by an internal monitoring body in section 1;
 2. deletes the following sentence “*or by the sponsor of the code of conduct, when the monitoring body is an inside body*” from requirement 1.1, third bullet point, or otherwise clarify it, so that the requirements of independence and impartiality, as set in the Guidelines, are met;
 3. adjusts the wording in requirement 1.3, in order to ensure that the funding of the monitoring body does not affect its independency;
 4. softens the wording of requirement 8.3, referring to the monitoring body’s responsibilities in a general manner so that this requirement appear less burdensome for small and medium entities applying for accreditation;
 5. specifies which information of the monitoring body’s report on annual activities is deemed relevant for publication, as well as the level of detail of information that needs to be included in such reports;
 6. includes the obligation to demonstrate independence in relation to the accountability of the monitoring body.
41. Regarding *transparent complaint handling* the Board recommends that the ES SA:
1. adopts a more flexible approach in requirement 5.2, regarding the timeline for resolving complaints;
 2. includes reference to remedies and corrective measures in requirement 5.2;

3. specifies the kind of relevant information that the monitoring body is obliged to publish with regards to the final decisions adopted.
42. Regarding *communication with the AEPD* the Board recommends that the ES SA:
1. rephrases requirement 6.2 in order to cover appropriate time expectations for the communication to the AEPD;
 2. deletes reference to the scope of accreditation or, alternatively, clarify the meaning thereof in requirement 6.2, fourth bullet point;
 3. adds reference to “exclusion” in requirement 6.3, for reasons of clarity.

43. Regarding *legal status* the Board recommends that the ES SA:
1. deletes reference to the “*legal personality*” in requirement 8.1 in order to clarify that internal monitoring bodies are not excluded;
 2. clarifies whether the monitoring body may have recourse to subcontractors and on which terms and conditions and that these are reflected in the requirements or explanatory notes. If subcontracting is allowed, amend the requirements or explanatory notes, so that the obligations applicable to the monitoring body are applicable in the same way to subcontractors.

4 FINAL REMARKS

44. This opinion is addressed to the Spanish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
45. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board
The Chair
(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 2/2020 on the Belgium data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 28 January 2020

Table of contents

1	Summary of the facts	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the BE accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	6
2.2.3	CONFLICT OF INTEREST	8
2.2.4	EXPERTISE.....	8
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	9
2.2.6	TRANSPARENT COMPLAINT HANDLING.....	9
2.2.7	COMMUNICATING WITH THE BE SA	10
2.2.8	CODE REVIEW MECHANISMS.....	10
2.2.9	LEGAL STATUS	10
3	CONCLUSIONS / RECOMMENDATIONS.....	11
4	FINAL REMARKS	12

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, to provide written guidance explaining the accreditation requirements; and, finally, requesting them to adopt these requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term ‘accreditation’. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

their proposed monitoring body meets the requirements set out in article 41 (2) to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Belgium Supervisory Authority (hereinafter "BE SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 25th October 2019.
2. In compliance with article 10 (2) of the Board Rules of Procedure,² due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
3. All accreditation requirements submitted to the Board for an opinion must fully address article 41(2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.

4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1)(p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.
5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to ‘encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.’ (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the BE SA to take further action.
8. This opinion does not reflect upon items submitted by the BE SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the BE accreditation requirements for Code of Conduct’s monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The Board notes that the draft accreditation requirements do not follow the structure set out in section 12 of the Guidelines. In order to facilitate the assessment and standardise the requirements, the Board recommends the BE SA to follow the structure of the Guidelines in the draft decision.
11. The Board notes that paragraph 3 of the introduction states that the monitoring body has to fulfil the accreditation requirements set out in the BE SA’s decision, in addition to the requirements of the GDPR and section 12 of the Guidelines. Whereas the reference to the Guidelines is welcomed, the Board notes that the BE SA’s requirements are not an addition to the ones established in the GDPR, but rather

a development thereof. The Board encourages the BE SA to amend the wording, in order to make clear that the requirements in the decision are not in addition to those in the GDPR, but based on those.

12. The Board observes the BE SA's draft accreditation requirements refer several times to "the number of code members". In this regard, the second paragraph of requirement 3.2 of the BE SA accreditation requirements states that the amount and type of human resources required depend on "...the number of code members". It is unclear how the assessment of the BE SA could be based on this criteria, considering that code member numbers might not be known when the monitoring body applies for accreditation and that may change considerably after the accreditation has been granted. Moreover, according to the Guidelines, resources and staffing of the monitoring body should be proportionate to the expected number and size of code members, amongst other elements (paragraph 73, page 24 of the Guidelines). The Board notes the same reference to 'number of code members' in requirements 5.2 and 6.2. Therefore the Board recommends the BE SA to include appropriate references to "the expected number and size of code of code members", to align the text with the Guidelines and allow for more flexibility.
13. Finally, the Board notes that there is no reference to the duration of the accreditation or accreditation withdrawal procedures. Whilst the Board accepts that these areas fall into the area of guidance supporting the accreditation requirements, the Board considers them important areas in terms of ensuring that the whole accreditation process is transparent. Therefore, the Board encourages the BE SA to clarify accreditation duration and withdrawal procedures in supporting guidance for the accreditation requirements.

2.2.2 INDEPENDENCE

14. The Board is of the opinion that independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. These rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, nor subject to any form of pressure that might affect its decisions. Therefore, the monitoring body must demonstrate impartiality and independence in relation to four main areas: legal and decision making procedures, financial resources, organisational resources and structure and accountability. The examples provided in the BE SA's accreditation requirements do not cover entirely the four areas outlined. The Board recommends the BE SA to further develop the requirements concerning impartiality and independence of the monitoring body, in line with the four areas. Furthermore, the Board encourages the BE SA to include practical examples that provide a clearer view on how the impartiality and independence can be demonstrated in the four areas.
15. The Board observes that the example given in requirement 1.1, third paragraph, last indent ("information on the contractual relationship between the monitoring body and the code owner") is only applicable to external monitoring bodies. Where the monitoring body is part of the code owner organisation, particular focus must be made on their ability to act independently. The Board encourages the BE SA to tailor the examples taking into account that monitoring bodies can be external or internal monitoring bodies.
16. Moreover, the Board considers that the last paragraph of requirement 1.1 could be clarified to explain how independence from the sector to which the code applies will be assessed, considering that such "sector" might be an indistinct entity. The Board encourages the BE SA to clarify the drafting, providing

for a better understanding of the concept and of the kind of evidence that the monitoring bodies can provide to comply with the requirement.

17. With regard to the accountability of the monitoring body, the Board notes that the monitoring body should be able to demonstrate “accountability” for its decisions and actions in order to be considered to be independent. The Board considers that the accountability requirements in section 9 of the BE SA’s accreditation requirements do not fully cover all the elements that should be taken into account. The BE SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. This could be accomplished through such things as setting out the roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the staff about the governance structures and the procedures in place. Thus, the Board recommends the BE SA to strengthen the requirements for accountability, to allow for a better understanding of its content in relation to the independence of the monitoring body, and offer more examples of the kind of evidence that the monitoring bodies can provide
18. Requirement 3.1 (section 3 “adequate human resources”) of the BE SA accreditation requirements establishes that the monitoring body shall demonstrate that it is *“able to freely choose qualified staff in order to fulfil its tasks”*. The Board notes that the monitoring body can also have staff that has been chosen by other body independent of the code, as stated in the Guidelines (paragraph 68, page 23). The Board recommends the BE SA to align the wording with the Guidelines, by adding the possibility that the staff is chosen by other body independent of the code. Furthermore, the Board is of the opinion that, from a practical point of view, some examples might also be helpful. An example of staff provided by a body independent of the code would be monitoring body personnel that have been recruited by an independent external company, which provides recruitment and human resources services. Therefore, the Board encourages the BE SA to add an example in line with the one provided in this paragraph.
19. Moreover, the Board notes that requirement 3.1 of the BE SA accreditation requirements does not explain how the monitoring body can demonstrate that it is able to freely choose qualified staff. In order to facilitate the practical implementation of the requirements, the Board considers that some examples would be helpful. Hence, the Board encourages the BE SA to clarify how the monitoring body can demonstrate its ability to freely choose qualified staff.
20. With regard to the obligation of the monitoring body to demonstrate that it is composed of an adequate number of staff (requirement 3.2 of the BE SA accreditation requirements), the Board considers that, from a practical point of view, some examples would be helpful. Therefore, the Board encourages the BE SA to clarify how the monitoring body can demonstrate that it is composed of an adequate number of staff.
21. The Board observes that requirement 4.3 of the BE SA accreditation requirements (section “financial arrangements”) requires that the monitoring body shall have “adequate arrangements in place (...) to cover potential financial penalties”. The Board is of the opinion that this obligation could prevent small or medium monitoring bodies from getting accredited. Therefore, the Board recommends the BE SA to either delete this requirement or to soften the wording and refer to the monitoring body’s responsibilities in general.

2.2.3 CONFLICT OF INTEREST

22. The Board observes that requirement 1.2 of the BE SA accreditation requirements only addresses the situations in which there is a conflict of interest related to the personnel of the monitoring body. The accreditation requirements should also reflect other scenarios where there might be conflicts of interest of the monitoring body itself, for example, due to its activities, relationships, organisation or procedures. Thus, the Board recommends the BE SA to amend the draft accreditation requirements to reflect that the conflict of interests shall be avoided also in relation to the monitoring body itself, and not only with regard to its staff.
23. Furthermore, the Board observes that the BE SA accreditation requirements do not explicitly include the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties and to not seek nor take instructions from any person, organisation or association (paragraph 68, page 23 of the Guidelines). Therefore, the Board recommends the BE SA to align the text with the Guidelines and include the above-mentioned obligations.

2.2.4 EXPERTISE

24. The Board notes that requirement 5.1 of the BE SA's expertise requirements include: knowledge and experience on data protection legislation, knowledge and experience in the sector or processing activity for which it will act as monitoring body as well as knowledge and experience in auditing to establish the monitoring body capacity to monitor compliance of the code members with the code of conduct.
25. Whilst the BE SA has included all the elements from the Guidelines in its requirements, the Board is of the opinion that the level of the knowledge and expertise in data protection issues should be aligned with the Guidelines. Therefore, the Board encourages the BE SA to align the text with the Guidelines, and require an in-depth understanding of data protection legislation.
26. The Board considers that the accreditation requirements need to be transparent. They also need to provide for monitoring bodies seeking accreditation in relation to codes that cover micro, small and medium-sized enterprises' processing activities (article 40 (1) GDPR).
27. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (in section 6.4 of the Guidelines), by demonstrating 'why their proposals for monitoring are appropriate and operationally feasible' (paragraph 41, page 17 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code's monitoring activities effectively. To that end, in order to evaluate the expertise level required by the monitoring body, it should, in general, be taken into account such factors as: the size of the sector concerned, the different interests involved and the risks of the processing activities addressed by the code. This would also be important if there are several monitoring bodies, as the code will help ensure a uniform application of the expertise requirements for all monitoring bodies covering the same code.
28. The expertise of each monitoring body should be assessed in line with the particular code. Therefore, the Board encourages the BE SA to take into account the additional expertise requirements that can be defined by the code and ensure that the expertise of each monitoring body is assessed in line with the particular code. Whereby the SA will verify if the monitoring body possess adequate competencies for the specific duties and responsibilities to undertake the effective monitoring of the code. The Board

also encourages the BE SA to redraft the requirement 5.2 following the same wording as other requirements, - i.e. start the requirement with ‘the monitoring body shall demonstrate that its...’

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

29. Requirement 6.2 of the BE SA’s accreditation requirements establishes that the criteria to carry out the audit plans include (underlined added) “the received number of complaints”. Whereas the number of complaints could be a relevant criterion, the Board considers that other elements, such as the focus of the complaints, may have a greater significance. Therefore, the Board encourages the BE SA to delete the reference to the “number” of complaints, and keep it more general, such as “the received complaints”.
30. The Board notes that requirement 6.3 of the BE SA accreditation requirements refers to a code of conduct as a tool for international transfers. As part of the work program for 2019-2020, the Board is currently working on Guidelines on Codes of Conduct as a tool for transfers. Since the Guidelines have not been adopted yet, the Board considers that the reference in requirement 6.3 of the BE SA accreditation requirements might create confusion and may need to be amended once the Guidelines are adopted. Therefore, the Board recommends the BE SA to delete requirement 6.3.

2.2.6 TRANSPARENT COMPLAINT HANDLING

31. The Board observes that the complaints procedure in requirement 7.1 is addressed only to data subjects, preventing other actors, such as organisations or associations representing data subjects or active in the field of the protection of personal data, to file a complaint with the monitoring body. The Board encourages the BE SA to amend the requirement in order to include a more comprehensive wording that does not limit the possibility to file a complaint only to data subjects.
32. Moreover, the Board notices that the BE SA accreditation requirements do not make any reference to the corrective measures that must be determined in the code of conduct, as per Article 40(4) GDPR. Therefore, the Board recommends the BE SA to add a reference to the list of sanctions set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.
33. The Board notes that requirement 7.3 of the BE SA accreditation requirements contains the duty of the monitoring body to make the register of the complaints received and their outcome available to the SA on request. Whereas the Board acknowledges the intention of the BE SA to comply with the transparency principle regarding the complaints handling procedure, the Board considers that the BE SA accreditation requirements should contain the obligation of the monitoring body to make the decisions, or general information thereof, publicly available, as provided in the Guidelines (paragraph 74, page 24). Therefore, the Board recommends the BE SA to align the text of the accreditation requirements with the Guidelines, in order to ensure that the decisions, or general information thereof, are publicly available.
34. Furthermore, where the BE SA decides to ensure the transparency of the complaints handling procedure by requiring that the monitoring body publishes summary information about the decisions taken in this context, the Board recommends that the BE SA specifies the kind of information that the monitoring body is obliged to publish. For example, the monitoring body could publish, on a regular basis, statistical data with the result of the monitoring activities, such as the number of complaints received, the type of infringements and the corrective measures issued.

2.2.7 COMMUNICATING WITH THE BE SA

35. With regard to the communication with the BE SA, requirement 8.1 establishes that the monitoring body will communicate to the BE SA “at periodic intervals”, any action taken in cases of code infringements and the reasons for such actions., alongside annual reporting, providing an overview of the monitoring body’s activities and decisions. Whilst the Board welcomes the explicit reference to the periodic communication with the SA and the criteria to determine its frequency, the Board considers that there should be an appropriate level of flexibility to help guide monitoring bodies as to when to report, rather than setting the criteria too rigidly; the criteria should take into account changing circumstances and different factors that are listed. The Board encourages the BE SA to redraft 8.1 to make it clear that the periodic reporting is flexible.
36. According to requirement 8.1, the frequency of the communication will depend on the “the risks for data subjects, the sensitivity and complexity of data processing that takes places within the context of the code of conduct, the size of the sector concerned and the number of code members”. In addition, the Board notes that the BE SA review of such reports would normally focus on the more serious or common infringements and the measures taken. The Board encourages the BE SA to make reference to the seriousness and frequency of infringements and to the measures taken, as part of the criteria to determine the frequency of communication with the SA. Furthermore, the Board encourages the BE SA to add a reference to the communication requirements as set by the Code of Conduct itself.
37. Furthermore, significant changes in the number of code members are not included in requirement 8.2 of the BE SA accreditation requirements, as a substantial change that shall be communicated to the SA without undue delay. Therefore, the Board recommends the BE SA to include relevant changes to the number of code members in the list of significant changes in requirement 8.2.
38. Turning to requirement 8.3, the Board supports the publicly available information, but considers that the wording for the last two bullets could be made clearer. To this end, the Board recommends the BE SA to add to the last two bullets a suitable reference to the rules and procedures as set out in the code itself.

2.2.8 CODE REVIEW MECHANISMS

39. The accreditation requirements contain the obligation of the monitoring body to contribute appropriately to the review of the code of conduct (requirement 11.2). The Board encourages accreditation requirements which require a monitoring body to develop mechanisms that enable feedback to the code owners and to any other entity referred to in the code of conduct. Some options would be to use the results of the audit process, the handling of complaints or actions taken in code infringement cases. Therefore, the Board encourages the BE SA to amend the draft, adding that the monitoring body must have mechanisms that enable feedback to the code owner and to any other entity referred to in the code of conduct.

2.2.9 LEGAL STATUS

40. According to requirement 2.4 of the BE SA accreditation requirements, the sustainability and continuity of the monitoring activities shall be demonstrated in relation to the “mechanisms to overcome the withdrawal of one or several code members”. The Board considers that it is unclear how the withdrawal of one or several code members would affect the performance of the monitoring body. Therefore, the Board encourages the BE SA to delete the above-mentioned reference.

41. Furthermore, with regard to the reference to “sufficient financial resources” in requirement 2.4 of the BE SA accreditation requirements, the Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. Thereby, the Board encourages that the BE SA amend the explanatory note, adding the above-mentioned reference to “procedures”.
42. Finally, regarding subcontractors, requirement 10.2 of the BE SA accreditation requirements states that “the monitoring body shall identify all of its subcontractors when it applies for accreditation.” The Board considers that the list of subcontractors is not as relevant as the actual tasks and role that they will carry out. Therefore, the Board encourages the BE SA to amend the wording, stating that the monitoring body will specify the tasks and roles that the subcontractors will carry out.

3 CONCLUSIONS / RECOMMENDATIONS

43. The draft accreditation requirements of the Belgian Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
44. As general remarks, the Board recommends that the BE SA
 1. follows the structure set out in section 12 of the Guidelines.
 2. includes appropriate references to “the expected number and size of code members” in requirements 3.2, 5.2 and 6.2, to align the text with the Guidelines and allow for more flexibility.
45. Regarding ‘independence’ the Board recommends that the BE SA:
 1. further develops the requirements concerning impartiality and independence of the monitoring body, in line with the four areas.
 2. strengthens the requirements for accountability, to allow for a better understanding of its content in relation to the independence of the monitoring body, and offer more examples of the kind of evidence that the monitoring bodies can provide.
 3. aligns the wording in requirement 3.1 to the Guidelines, by adding that the monitoring body can also have staff that has been chosen by other body independent of the code.
 4. either deletes requirement 4.3 or softens the wording and refers to the monitoring body’s responsibilities in general or clarifies the monitoring body’s responsibilities in reference to article 83.4 c) if the GDPR.
46. Regarding ‘conflict of interest’ the Board recommends that the BE SA:
 1. amends the draft accreditation requirements to reflect that the conflict of interests shall be avoided also in relation to the monitoring body itself, and not only with regard to its personnel.
 2. aligns the text with the Guidelines and includes the obligation of the monitoring body to refrain from any action that is incompatible with its tasks and duties and to not seek nor take instructions from any person, organisation or association
47. Regarding ‘established procedures and structures’ the Board recommends that the BE SA:

1. deletes requirement 6.3.
48. Regarding ‘transparent complaint handling’ the Board recommends that the BE SA:
1. adds a reference to the list of sanctions set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it
 2. aligns the text of the accreditation requirements with the Guidelines, in order to ensure that the decisions, or general information thereof, are publicly available.
 3. specifies the kind of information the monitoring body is obliged to publish in case the BE SA decides to ensure the transparency of the complaints handling procedure by requiring that the monitoring body publishes summary information about the decisions taken in this context.
49. Regarding ‘communication with the BE SA’ the Board recommends that the BE SA:
1. includes in the list of significant changes in requirement 8.2 a suitable reference to ‘changes in the number of code members’ .
 2. adds to the last two bullets of requirement 8.3 a suitable reference to the rules and procedures as set out in the code itself.

4 FINAL REMARKS

50. This opinion is addressed to the Belgium supervisory authority and will be made public pursuant to Article 64 (5)(b) GDPR.
51. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 3/2020 on the France data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 28 January 2020

Table of contents

1	Summary of the facts	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the FR accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	7
2.2.3	CONFLICT OF INTEREST	8
2.2.4	EXPERTISE.....	8
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	9
2.2.6	TRANSPARENT COMPLAINT HANDLING.....	10
2.2.7	COMMUNICATING WITH THE FR SA	11
2.2.8	CODE REVIEW MECHANISMS.....	11
2.2.9	LEGAL STATUS	11
3	CONCLUSIONS / RECOMMENDATIONS.....	12
4	FINAL REMARKS	13

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018, as last modified and adopted on 10 September 2019

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41 GDPR. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, to provide written guidance explaining the accreditation requirements; and, finally, requesting them to adopt these requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term ‘accreditation’. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

their proposed monitoring body meets the requirements set out in article 41 (2) to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The France Supervisory Authority (hereinafter "FR SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 25th October 2019.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
3. All accreditation requirements submitted to the Board for an opinion must fully address article 41(2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1)(p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to ‘encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking into account the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises’ (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the FR SA to take further action.
8. The Board notes that the document submitted by FR SA contains not only the accreditation requirements, but also explanatory notes, which include general and specific explanations about the FR SA’s approach to accreditation requirements.
9. This opinion does not reflect upon items submitted by the FR SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the FR accreditation requirements for Code of Conduct’s monitoring bodies

10. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct,

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

11. The Board notes that the draft accreditation requirements do not completely follow the structure set out in Section 12 of the Guidelines. In order to facilitate the assessment and standardise the requirements, the Board recommends the FR SA to follow the structure of the Guidelines in the draft decision.
12. The Board observes that the draft requirements refer repeatedly to the auditing activities of the monitoring body and other related terms, such as “auditors” and “audit mission” (e.g. sections 1.1,

3.2, 4, 5, 8 and 9). The Board is of the opinion that the monitoring activities are not limited to audit, since they can be performed in different ways. On the same line, the staff of the monitoring body will not necessarily be auditors, due to the different kind of tasks that the monitoring body performs. Therefore, the Board recommends the FR SA to change the references to “audit” and related terms, in order to reflect the broader spectrum of activities that can be performed by the monitoring body.

13. The Board notes that, in page 3 of the draft decision, the FR SA establishes that the accreditation term will be initially set at three years, after which there will be a review of the accreditation that might result in the loss of the accreditation. The Board observes that the sentence might be understood as if the review of the accreditation requirements only takes place every three years. The Board notes that article 41 GDPR does not refer to the validity of the accreditation of a monitoring body and that there is a margin of manoeuvre for the national SAs. Moreover, the Board notes that the accreditation requirements should be re-assessed periodically, in order to ensure compliance with the GDPR. Indeed, even if the requirements establish a time limit for the accreditation of the MB, this is to be considered without prejudice of the exercise, at any time, of the SA’s supervisory powers with regard to the obligations of the MB. Therefore, for the sake of clarity, the Board encourages the FR SA to clarify that the requirements may be reviewed periodically and to provide transparent information on what happens after the expiry of the validity of the accreditation and what the procedure will be.
14. The Board notes that, in requirement 1.4, the example given as a “supporting element” refers to a “model of service agreement used between monitoring body and the member of the code of conduct” and to a “template of non-disclosure agreement”. The Board highlights that the binding nature of the rules of the code of conduct, including those providing for the monitoring mechanism, would result from the adhesion of the code members to the code as well as from their membership of the representative association. Whereas contractual arrangements are not, *per se*, excluded, the Board is of the opinion that the essential elements of the monitoring body’s function should be included in the code itself. Additional clauses may be added in the form of an agreement or contract between the monitoring body and the code member, as long as they do not entail a variation in the essential elements of the monitoring body’s function, as set out in the code. Therefore, the Board recommends the FR SA to specify that the core elements of the monitoring body’s function will be included in the code of conduct.
15. Moreover, the Board observes that, according to requirement 1.4, the documents relating to the performance of the MB’s duties are destroyed “if they are no longer of use after the audit”. This could be misleading, since there might be a need to keep such documents for different reasons after they are no longer of use, such as to meet legal obligations. Therefore, the Board encourages the FR SA to amend the requirement in order to take into account other possible legal obligations or other legitimate reasons requiring to keep the documents after they are no longer of use.
16. The Board notes that requirement 1.5 establishes that the monitoring body *“shall ensure when carrying out its missions, that complies with the security measures the code member provides”*. The Board considers that the reference to “security measures” needs further detail, especially with regard to its relation to data protection. Moreover, the Board highlights that the security measures cannot prevent or restrict the monitoring body from carrying out its duties fully. Therefore, the Board encourages the FR SA to clarify the concept of “security measures” in relation to data protection, and to specify that the security measures in place cannot prevent the monitoring body from carrying out its duties.

2.2.2 INDEPENDENCE

17. With regard to the independence of the monitoring body, requirement 1.3 provides that (underline added) “the monitoring body shall demonstrate that all appropriate human, financial and material resources in proportion with the code of conduct's scope are used”. In accordance with the Guidelines, the resources of the monitoring body should be proportionate “to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing” (paragraph 73, page 24 of the Guidelines). Thus, the Board encourages the FR SA to align the text of the requirement 1.3 to the Guidelines by adding the above-mentioned reference.
18. As for the financial independence of the monitoring body (requirement 2.2), the Board considers that the requirement would benefit from the addition of more details, in order to make clear that the means by which the monitoring body obtains financial support should not adversely affects its independence, and that it should have the financial stability and resources necessary for the effective performance of its tasks. For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the FR SA to define in the draft accreditation requirements what constitutes financial independence, and to provide some examples.
19. Moreover, the Board notes that the requirement does not differentiate between internal and external monitoring bodies. Where the monitoring body is part of the code owner organisation, particular focus must be made on their ability to act independently. The Board encourages the FR SA to make such a distinction and to add examples that demonstrate how independence can be achieved in both cases.
20. Finally, the Board notices that the FR SA refers to functional independence, without further specifying how it can be demonstrated. Thus, the Board encourages the FR SA to define the content of functional independence and to explain how the monitoring body can demonstrate its independence when performing its duties.
21. The Board observes that the draft accreditation requirements do not contain any reference to the organisational independence of the monitoring body. The Board notes that monitoring bodies should have the human and technical resources necessary for the effective performance of their tasks. Monitoring bodies should be composed of an adequate number of personnel so that they are able to fully carry out the monitoring functions, reflecting the sector concerned and the risks of the processing activities addressed by the code of conduct. Personnel of the monitoring body shall be responsible and shall retain authority for their decisions regarding the monitoring activities. These organisational aspects could be demonstrated through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel, as well as the duration of the personnel's mandate, contract or other formal agreement with the monitoring body. Moreover, the draft requirements should clearly state that the monitoring body shall be independent in performing its tasks and exercising its powers (paragraph 67, page 22 of the Guidelines). Therefore, the Board recommends the FR SA to provide suitable requirements for the organisational aspects of the independence of the monitoring body and add the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines
22. Furthermore, the Board notes that the monitoring body should be able to demonstrate “accountability” for its decisions and actions in order to be considered to be independent. This could

be accomplished through such things as setting out the roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the staff about the governance structures and the procedures in place. Therefore, the Board recommends the FR SA to include requirements that suitably address the accountability of the monitoring body.

2.2.3 CONFLICT OF INTEREST

23. The Board notes that the requirements regarding conflict of interest (section 3 of the draft accreditation requirements), do not include all the elements of the Guidelines. Specifically, the monitoring body shall remain free from any external influence and, therefore, it shall not seek nor take instructions from any person organisation or association. Moreover, the monitoring body should have its own staff (paragraph 68, page 23 of the Guidelines). The EDPB recommends the FR SA to include the above-mentioned elements, thus aligning the text with the Guidelines.
24. The Board observes that there is no reference to internal monitoring bodies, which should be appropriately protected from any sort of sanctions or interference by the code owner, other relevant bodies, or members of the code, as a consequence of the fulfilment of its tasks (paragraph 68, page 23 of the Guidelines). The Board encourages the FR SA to provide examples that include internal monitoring bodies.
25. Requirement 3.2 of the FR SA accreditation requirements establishes that the monitoring body shall “provide a procedure to anticipate and deal with any situation likely to create a conflict of interest.” The Board considers that the measures and procedures in place aiming at preventing conflicts of interest should ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties. Therefore, the Board recommends that the FR SA includes in the accreditation requirements that the procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.

2.2.4 EXPERTISE

26. The Board observes that the FR SA’s expertise requirements in section 4 refer only to “auditors” and the “audit team” of the monitoring body, without further clarifying the concept. As stated above, the reference to only the auditing activities of the monitoring body does not cover the broader spectrum of the activities it can carry out. Moreover, the FR SA’s expertise requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. The Board recommends that the FR SA replaces the reference to “auditors” for a more suitable one, such as “staff carrying out the monitoring activities or making decisions on behalf of the monitoring body”.
27. Turning to the level of expertise required, the Board considers that the accreditation requirements need to be transparent and to provide for monitoring bodies seeking accreditation in relation to codes that cover micro, small and medium-sized enterprises’ processing activities (article 40 (1) GDPR).
28. As required by the Guidelines, every code must fulfil the monitoring mechanism criteria (in section 6.4 of the Guidelines), by demonstrating ‘why their proposals for monitoring are appropriate and operationally feasible’ (paragraph 41, page 17 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code’s monitoring activities effectively. To that end, in order to evaluate the expertise level required by the monitoring body, it should, in general, be taken into account such factors as: the size of the sector concerned, the different interests involved and the risks of the

processing activities addressed by the code. This would also be important if there are several monitoring bodies, as the code will help ensure a uniform application of the expertise requirements for all monitoring bodies covering the same code.

29. In this regard, the Board considers that requirement 4.1.4 of the FR SA's accreditation requirements should include all the elements of the Guidelines, and in particular, the expertise in relation to the specific processing activities that are the subject matter of the code, and an in-depth understanding of data protection issues, in relation to the specific sector of the code. The Board recommends the FR SA to add the above-mentioned references, in line with the Guidelines. Moreover, the Board notes that the example provided as a supporting element refers only to "skills". The Board encourages the FR SA to redraft the example and refer to "knowledge and experience", instead of "skills".
30. The Board notes that requirement 4.1.5 refers to a "specific training on data protection", without providing further details. The Board is of the opinion that such a reference does not provide enough clarity about the expected knowledge in data protection that the monitoring body shall demonstrate. Thus, the Board encourages the FR SA to complete the reference to the data protection training with a reference to an adequate knowledge of data protection law, in line with the Guidelines.
31. Furthermore, the Board considers that the reference, in requirement 4.2.2, to the two years of professional experience for the legal personnel may curtail the freedom of the code owner to define the specific expertise requirements in the code of conduct (see paragraph 29 above). The Board encourages the FR SA to include a more general reference that takes into account the different types of codes, such as "a relevant level of experience in the field of data protection in accordance with the code itself". Moreover, the Board encourages the FR SA to take into account the additional expertise requirements that can be defined by the code, by including that reference in the text of the requirements, and to ensure that the expertise of each monitoring body is assessed in line with the particular code. Whereby the SA will verify if the monitoring body possess adequate competencies for the specific duties and responsibilities to undertake the effective monitoring of the code.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

32. The Board notes that on requirement 5.4 (section on "requirements relating to the audit process"), the audit procedure plans refer to the assessment for eligibility of controllers and processors to apply the code and to monitor compliance after adhesion. It also states that the procedure takes every change to the conduct of conduct into account. However, there is no reference to the review of the code's operation. The Board highlights that the accreditation requirements should specifically contain the obligation of the monitoring body to have governance structures to carry out reviews of the code's operation (paragraph 70, page 23 of the Guidelines). The Board recommends the FR SA include the reference to the review of the code's operation, in line with the Guidelines.
33. Requirement 5.5 of the FR SA's accreditation requirements establishes that the criteria to carry out the audit program include "the number of code of conduct members to be monitored and the geographical scope". The Board considers that a more comprehensive wording would also include the risk associated with the data processing and the received complaints. The Board encourages the FR SA to add the above-mentioned references.
34. The Board notes that requirement 5.6 of the FR SA's accreditation requirements states that "The audit procedure ensures that each mission is prepared and framed by instructions [...]" . The Board considers that the current wording may lead to confusion as to whether the monitoring body will conduct the

audit in an independent manner. Moreover, the reference to the “audit mission” in the supporting elements could be misleading, since the monitoring procedure can be shaped in different ways (i.e. random or unannounced audits, annual inspections, regular reporting and the use of questionnaires). Therefore, the Board encourages the FR SA to redraft the requirement, to make clear that the audit will be carried out in an independent manner and in different ways.

35. The Board welcomes the obligation to provide feedback to the audited code member, included in requirements 5.7 and 5.9. However, the Board considers too restrictive to include as a requirement the manner in which the feedback shall be given. The Board encourages the FR SA to redraft the requirement and include the manner in which the feedback shall be given as an example. Moreover, the difference between requirement 5.7 and requirement 5.9 is not clear. The Board encourages the FR SA to clarify the difference between the two requirements.

2.2.6 TRANSPARENT COMPLAINT HANDLING

36. Regarding the complaints about code members (requirement 6.3 of the FR SA accreditation requirements), the Board acknowledges that complaints handling process requirements should be set at a high level and reference reasonable time frames for answering complaints. In this regard, the Board notes that the FR SA accreditation requirements state, in the supporting elements, that the reasonable timeframe to process complaints should not exceed three months. The Board considers this time limit too restrictive and difficult to comply with in practice. Thus, the Board recommends the FR SA to take a more flexible approach, by stating that the monitoring body will have to provide the complainant with progress reports or the outcome within a reasonable timeframe, such as three months.
37. The Board notes that requirement 6.2 of the FR SA accreditation requirements states that the complaint handling procedure will be accessible and easily understood by all data subjects and the public. The Board acknowledges that this wording is based on the Guidelines. Nonetheless, the Board is of the opinion that, for the sake of clarity, the requirements should specify the meaning of “public” and whether it also includes code members. Therefore, the Board encourages the FR SA to amend requirement 6.2 accordingly.
38. The Board notes that requirement 6.4 of the FR SA accreditation requirements contains the duty of the monitoring body to keep the record of the processing of all complaints received readily available to the SA, who may access it at any time. Whereas the Board acknowledges the intention of the FR SA to comply with the transparency principle regarding the complaints handling procedure, the Board considers that the FR SA accreditation requirements should contain the obligation of the monitoring body to make the decisions, or general information thereof, publicly available, as provided in the Guidelines (paragraph 74, page 24). Therefore, the Board recommends the FR SA to align the text of the accreditation requirements with the Guidelines, in order to ensure that the decisions, or general information thereof, are publicly available. In addition, where the FR SA decides to ensure the transparency of the complaints handling procedure by requiring that the monitoring body publishes summary information about the decisions taken in this context, the Board recommends that the FR SA specifies the kind of information the monitoring body is obliged to publish. For example, the monitoring body could publish, on a regular basis, statistical data with the result of the monitoring activities, such as the number of complaints received, the type of infringements and the corrective measures issued.

2.2.7 COMMUNICATING WITH THE FR SA

39. With regard to the communication with the FR SA about measures taken by the monitoring body, requirement 7.3 of the FR SA accreditation requirements establishes that the monitoring body will inform the FR SA “without undue delay and in writing, as soon as a binding measure is taken against one of code of conduct member”. The Board considers that the monitoring body shall communicate periodically with the SA, and that the frequency of the communication would depend on several criteria, including the seriousness of the infringement and the measures taken. However, the Board is of the opinion that the communication to the SA “without undue delay” should be limited to those cases in which the measure taken is very serious, for example, the suspension or exclusion of a code member (as specified in requirements 7.4 and 7.5 of the FR SA accreditation requirements). Otherwise, it could be very burdensome for the monitoring body and for the competent SA. Therefore, the Board recommends the FR SA to delete the reference to “without undue delay” and adopt a more flexible approach, which allows for periodic communication with the SA, based on several criteria, including the seriousness of the infringement and the measure adopted and to modify accordingly the example in the “supporting elements” cell.
40. The Board notes that section 9.1 establishes that the monitoring body will ensure that the summaries of all audits carried out are at the disposal of the FR SA. The reference to the audits does not cover all the range of activities carried out by the monitoring body and the actions taken. Whereas the Board acknowledges that the reference to the “audit” might be due to the translation of the term, the Board recommends the FR SA to amend the wording in order to make clear that the monitoring body will have, at the disposal of the FR SA, the summaries of all actions taken.

2.2.8 CODE REVIEW MECHANISMS

41. The Board observes that the FR SA’s accreditation requirements do not contain all the necessary elements to ensure that the code remains relevant and continues to contribute to the proper application of the GDPR. The Board notes that it is the role of the code owner to ensure the continued relevance and compliance of the code of conduct with applicable legislation. Whilst the monitoring body is not responsible to carry out that task, it shall contribute to any review of the code. As a result, the Board recommends the FR SA to provide accreditation requirements that make clear that the monitoring body will contribute to any review of the code.

2.2.9 LEGAL STATUS

42. The code of conduct itself will need to demonstrate that the operation of the code’s monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that a monitoring body demonstrates that it can deliver the code of conduct’s monitoring mechanism over a suitable period of time. The financial, human and material resources to ensure the continuity of the monitoring body should be accompanied with the necessary procedures to ensure the functioning of the monitoring mechanism over a suitable time. Therefore, the Board recommends FR SA to explicitly require that monitoring bodies shall demonstrate continuity of the monitoring function over time. The Board also encourages the FR SA to include in the accreditation requirements that, in order to demonstrate the continuity of the monitoring function, the monitoring body should demonstrate that it has sufficient financial and other resources, and the necessary procedures.
43. The Board notes that the FR SA’s accreditation requirements allow for the use of subcontractors (Section 8 of the FR SA’s accreditation requirements). However, the requirements do not expressly

state that outsourcing does not lead to a delegation of responsibility for the monitoring body, and that the monitoring body remains responsible to the SA for monitoring in all cases. The Board recommends that the FR SA indicates that the monitoring body remains responsible to the SA for monitoring in all cases.

44. The Board considers that the explanatory for Section 8 is too general and does not provide additional information that would be helpful to have a better understanding of Section 8. Moreover, it assumes that subcontractors will always be processors, whereas that is not the case in all situations. Therefore, the Board encourages the FR SA to add more details to the explanatory note in accordance with the different sections and to modify the wording regarding the role of the subcontractors, in order to avoid misunderstandings.

3 CONCLUSIONS / RECOMMENDATIONS

45. The draft accreditation requirements of the France Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
46. As general remarks, the Board recommends that the FR SA:
1. follows the structure set out in section 12 of the Guidelines.
 2. changes the references to “audit” and related terms, in order to reflect the broader spectrum of activities that can be performed by the monitoring body.
 3. with regard to the contract referred to in requirement 1.4, specifies that the core elements of the monitoring body’s function will be included in the code of conduct.
47. Regarding ‘independence’ the Board recommends that the FR SA:
1. provides suitable requirements for the organisational aspects of the independence of the monitoring body and add the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.
 2. includes a reference to the accountability of the monitoring body.
48. Regarding ‘conflict of interest’ the Board recommends that the FR SA:
1. aligns the text with the Guidelines, by including the obligation of the monitoring body to remain free from any external influence and to not seek nor take instructions from any person organisation or association, and that the monitoring body should have its own staff.
 2. includes in the accreditation requirements that the procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.
49. Regarding ‘expertise’ the Board recommends that the FR SA:
1. replaces the reference to “auditors” for a more suitable one, such as “personnel carrying out the monitoring activities or making decisions on behalf of the monitoring body”.

2. aligns the text with the Guidelines, by adding, in requirement 4.1.4, the expertise in relation to the specific processing activities that are the subject matter of the code, and an in-depth understanding of data protection issues, in relation to the specific sector of the code.
50. Regarding ‘established procedures and structures’ the Board recommends that the FR SA:
1. includes the reference to the review of the code’s operation, in line with the Guidelines.
51. Regarding ‘transparent complaint handling’ the Board recommends that the FR SA:
1. takes a more flexible approach, by stating that the monitoring body will have to provide the complainant with progress reports or the outcome within a reasonable timeframe, such as three months.
 2. aligns the text of the accreditation requirements with the Guidelines, in order to ensure that the decisions, or general information thereof, are publicly available.
 3. specifies the kind of information the monitoring body is obliged to publish in case the FR SA decides to ensure the transparency of the complaints handling procedure by requiring that the monitoring body publishes summary information about the decisions taken in this context.
52. Regarding ‘communicating with the FR SA’ the Board recommends that the FR SA:
1. deletes the reference to “without undue delay” and adopts a more flexible approach, which allows for periodic communication with the SA, based on several criteria, including the seriousness of the infringement and the measure adopted and modifies accordingly the example in the “supporting elements” cell.
 2. amends the requirement in order to include a summary of all the actions taken by the monitoring body, which should be at the disposal of the FR SA.
53. Regarding ‘code review mechanisms’ the Board recommends that the FR SA:
1. provides accreditation requirements that make clear that the monitoring body will contribute to any review of the code.
54. Regarding ‘legal status’ the Board recommends that the FR SA:
1. explicitly requires that monitoring bodies shall demonstrate continuity of the monitoring function over time.
 2. indicates that the monitoring body remains responsible to the SA for monitoring in all cases.

4 FINAL REMARKS

3. This opinion is addressed to the France supervisory authority and will be made public pursuant to Article 64 (5)(b) GDPR.
4. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its

draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 4/2020 on the draft decision of the competent supervisory authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 29 January 2020

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX (Section 0 of the draft additional accreditation requirements).....	6
2.2.2	GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft additional accreditation requirements)	6
2.2.3	RESOURCE REQUIREMENTS (Section 6 of the draft additional accreditation requirements).....	7
2.2.4	PROCESS REQUIREMENTS, ARTICLE 43(2)(C),(D) (Section 7 of the draft additional accreditation requirements)	7
3	Conclusions / Recommendations.....	8
4	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter “GDPR”),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter “Law Enforcement Directive”).

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

(4) The “Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)” (hereinafter the “Guidelines”), and “Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679” will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The UK SA has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. Following a decision deeming the file complete, it was broadcasted on 25 October 2019. The UK national accreditation body (NAB), UKAS, will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the SA, once they are approved by the SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation

² Para. 39 Guidelines:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the UK SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

4. This assessment of UK SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably the Annex. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The guidelines Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines. Where this Opinion remains silent on a specific section of the UK SA's draft accreditation requirements, it should be read as the Board not having any comments and is not asking the UK SA to take further action.
9. This opinion does not reflect upon items submitted by the UK SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body

- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
 - f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
 - g. transparent handling of complaints about infringements of the certification.
10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
 - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
 - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
 - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
 - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

[2.2.1 PREFIX \(Section 0 of the draft additional accreditation requirements\)](#)

11. The Board acknowledges the fact that terms of cooperation, regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.
12. The Board takes note of the fact that the UK SA is putting in place such terms of cooperation with its NAB and that said terms will be made available on the website of the UK SA once finalised.

[2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION \(Section 4 of the draft additional accreditation requirements\)](#)

13. Concerning the requirement of legal responsibility (subsection 4.1.1), the Board takes note of the fact that the UK SA requires that the Certification Body (CB) being accredited "*should be able to provide evidence of compliance as required during the accreditation process*" with the GDPR and the UK Data Protection Act 2018. In order to ensure an adequate assessment and implementation of this

requirement, the Board encourages the UK SA to replace “*should be able to provide evidence*” by “*shall provide evidence*”. Therefore, the Board recommends that the UK SA amends the draft accordingly.

14. Concerning the certification agreement (subsection 4.1.2) and, in particular, requirement number 8, (number 9 in the Annex) the Board takes note of the fact that the UK SA created a reworded version of part of the requirement foreseen in Annex 1 of the Guidelines. The UK SA, however, omitted a reference to [where applicable] “the consequences for the customer should also be addressed”. The Board therefore recommends the UK SA to add the missing part of the requirement mentioned above.
15. Concerning the use of data protection seals and marks (subsection 4.1.3), the Board notes that the UK SA requests that a copy “*of the seal/mark/logo should be provided to the ICO for their records*.” Given that seals, marks and logos are handled not only by the certification body, but also by the scheme owner, the Board encourages the UK SA to refer also to any seals, marks and logos foreseen in any UK SA-approved certification schemes.

[2.2.3 RESOURCE REQUIREMENTS \(Section 6 of the draft additional accreditation requirements\)](#)

16. Concerning certification body personnel (subsection 6.1) and, in particular, point 6, the Board takes note of the fact that the UK SA has foreseen that “*Personnel responsible for certification decisions must have significant professional experience in identifying and implementing data protection measures*”. However, the Board considers that, while personnel making certification decisions may not have experience in “*significant professional experience in identifying and implementing data protection measures*” themselves, they should at least have access to someone with that expertise in order to make an informed decision. Significant professional experience in implementing such measures, at least in the early stages, would probably not be so widespread in this sector. Therefore, the Board encourages the UK SA to require that the certification body defines and explains the professional experience requirement which are appropriate to the certification scheme..

[2.2.4 PROCESS REQUIREMENTS, ARTICLE 43\(2\)\(C\),\(D\) \(Section 7 of the draft additional accreditation requirements\)](#)

17. Concerning the general subsection on process requirements (subsection 7.1) and, in particular, paragraph 4, the Board takes note of the additional requirement for an accreditation body to ensure that the certification body carries out an investigation or audit in cases where the data protection compliance is brought into question. The Board understands that the data protection compliance refers to the certification holder. However, this should be clearly specified in the requirements. Moreover, the Board considers that the UK SA should detail that such investigation should be linked with the scope of certification and the target of evaluation. Therefore, the Board recommends that the UK SA amends its requirement accordingly, by stating clearly that the data protection compliance refers to the certification holder and by specifying that the investigation should be linked with the scope of certification and the target of evaluation.
18. Concerning the application of process requirements (subsection 7.2), the Board takes note of the need for a certification body to specify “*whether processors are used, and when processors are the applicant, their responsibilities and tasks shall be described, and the application shall contain the relevant controller / processor contract(s)*.” While acknowledging that the UK SA has used the wording

of Annex 1, the Board encourages the UK SA to consider whether a reference to joint controllers and their specific arrangements should also be mentioned in this case.

19. Concerning evaluation methods (subsection 7.4), the Board takes note of the additional requirement foreseen by the UK SA requiring that, "*In addition to item 7.4.5 of ISO17065, it shall be provided that existing certification, which relates to the same object of certification, may be taken into account as part of a new evaluation [...]*". In this respect, the Board considers that it is necessary to further clarify that, in cases where existing certification is taken into account as part of a new evaluation, the scope of said certification should also be assessed in detail in respect of its compliance with the relevant certification criteria. Therefore, the Board encourages the UK SA to clarify the wording accordingly.
20. Concerning the sentence "*The complete evaluation report or information enabling an evaluation of the previous certification activity and its results can be considered.*" the Board recommends to the UK SA that "can" is replaced by "shall" where the certification body decides to take into account existing certification. In addition, the Board considers that it would be clearer to refer simply to "certification" rather than "certification activity" and recommends the UK SA to amend the draft accordingly. Moreover, the reference to the "previous certification" could be misleading, since it does not clearly refer to the existing certification the certification body wants to take into account as part of its own evaluation. The Board encourages the UK SA to change the wording, in order to clarify that the reference is to the existing certification. Finally, the Board notes that the certification body should be able to access the evaluation report and any other relevant information enabling an evaluation of the certification activity, in order to be able to take an informed decision. Therefore, the Board encourages the UK SA to clarify the wording accordingly.
21. Furthermore, in the paragraph starting with "*in addition to item 7.4.6 of ISO 17065*", the Board considers that, where the UK SA refers to "its certification mechanism", it actually meant "the certification scheme". Therefore, it recommends to the UK SA to replace the wording accordingly.
22. Regarding the changes affecting certification (subsection 7.10) and, in particular, the fourth bullet point ("decisions of the European Data Protection Board") the Board acknowledges that the UK SA has used the wording foreseen in Annex 1. However, in order to ensure a clear understanding of what is meant by "decisions of the European Data Protection Board", the Board encourages the UK SA to clarify the reference. An example could be to refer to "documents adopted by the European Data Protection Board".

3 CONCLUSIONS / RECOMMENDATIONS

23. The draft accreditation requirements of the United Kingdom Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
 24. Regarding 'general requirements for accreditation' the Board recommends that the UK SA:
 1. replaces, in subsection 4.1.1, the sentence "should be able to provide evidence" by "shall be able to provide evidence".
 2. includes in subsection 4.1.2 the missing part of the requirement, to align it with the text of the Annex 1 of the Guidelines.

25. Regarding ‘process requirements’ the Board recommends that the UK SA:
1. amends subsection 7.1. in order to make clear that the data protection compliance refers to the certification holder and that the investigation should be linked with the scope of certification and the target of evaluation
 2. amends subsection 7.4 replacing “can” by “shall” and “certification activity” by “certification”.
 3. replaces the reference to “certification mechanism” by “certification scheme”.

4 FINAL REMARKS

26. This opinion is addressed to the UK SA and will be made public pursuant to Article 64 (5)(b) GDPR.
27. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 5/2020 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 29 January 2020

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft accreditation requirements.	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	GENERAL REMARKS.....	6
2.2.2	GENERAL REQUIREMENTS FOR ACCREDITATION	6
2.2.3	RESOURCE REQUIREMENTS	7
2.2.4	PROCESS REQUIREMENTS.....	7
3	Conclusions / Recommendations.....	8
4	Final Remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

(4) The “Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)” (hereinafter the “Guidelines”), and “Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679” will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The LU SA has submitted its draft accreditation requirements under Article 43 (1)(a) to the EDPB. Following a decision deeming the file complete, it was broadcasted on 25 October 2019. The LU SA will perform accreditation of certification bodies to certify using GDPR certification criteria.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft accreditation requirements

The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in addition to ISO 17065 or as a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the LU SA is tasked

² Para. 39 Guidelines:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

by national law to carry out the accreditation of certification bodies. To this end, the LU SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.

The assessment of the accreditation requirements is aimed at examining variations (additions or deletions) from the Guidelines and notably the Annex. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact a consistent approach regarding the accreditation of certification bodies.

It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The guidelines Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.

The Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines. When this Opinion remains silent on a specific section of the LU SA's draft accreditation requirements, it should be read as the Board is not having any comments and is not asking the LU SA to take further action. The Board notes that the LU SA has provided information to help the assessment of the draft accreditation requirements. However, the Opinion of the Board only addresses the draft accreditation requirements.

Furthermore, this opinion does not reflect upon items submitted by the LU SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

3. Taking into account that:

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;

- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority.
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself,
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3)

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

- 4. The Board notes that the draft accreditation requirements do not completely follow the structure set out in Annex 1 to the Guidelines. For example, the sections on “scope” and “terms and definitions” are missing. In connection to this, the Board notes that some terms are not used consistently throughout the document, such as “client” and “applicant”. In order to avoid confusion, the terms used should be aligned with the Guidelines and the Annex definitions where possible and used consistently. Therefore, with the aim to facilitate the assessment, the Board encourages the LU SA to follow the structure of Annex 1 [to the Guidelines] in the draft accreditation requirements and add the missing sections..
- 5. The Board observes that, throughout the document, there are several references to the requirements “of this certification mechanism” (for example requirement 4.6.4) or to certification bodies that are accredited “under the (...) certification mechanism” (for example requirement 2.2.2). The reference to the certification mechanism seems to be a drafting issue. Thus, the Board encourages the LU SA to redraft the references in order to reflect that the certification bodies are accredited against the requirements approved by the supervisory authority.
- 6. On a similar note, the reference to the “requirements set out in this certification mechanism”, used throughout the document (for example requirement 1.1.1.2), is confusing. A more appropriate reference could be “the criteria set out in the certification mechanism”. Thus, the Board encourages the LU SA to clarify all references to “the certification mechanism” throughout the document.
- 7. The Board observes that several requirements (e.g. 3.2.1.1 and 4.1.2) refer to the “relevant International Standards”, the “relevant standard” or the “specified standard”. However, there is no definition of such standards and, therefore, it is unclear which are the standards referred to. Thus, the Board recommends the LU SA to clarify the meaning of such standards. This could be done, for example, in the “scope” or “terms and definitions” sections.

2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

- 8. The Board notes that LU SA requirement 1.1.1.1 refers to another standard (“ISAE 3000”), which the EDPB has not assessed. Therefore, the Board recommends the LU SA to clarify that the requirements cannot be overridden by any external standard, such as ISAE 3000.
- 9. The Board notes that the requirements in 1.6 do not include the obligation of the certification body to publish and make easily publicly available all versions of the approved criteria and all certification procedures, as established in the Annex to the Guidelines (section 4.6). The Board notes that LU SA

might be the certification scheme owner , however the Board considers that it would be helpful to add an appropriate reference to ensure that the criteria is up to date and easily accessible via the certification body itself. In this regard, the Board considers that by making the information available only upon request, as set up in requirement 1.6.1, the LU SA is establishing a stricter requirement than the Annex, which establishes that the information shall be make easily publicly available. Therefore, the Board recommends the LU SA to amend the requirement in order to include the obligation of the certification body to make easily publicly available all versions of the approved criteria and all certification procedures, in line with the Annex to the Guidelines.

10. The Board notes that requirement 1.2.4 refers to the 'certified process'. The Board considers that more precise wording, in line with the Guidelines could be used, such as 'certified processing operations/activities'. This provides for the broader certification scope, as provided by GDPR. Therefore, the Board encourages de LU SA to amend the draft requirements accordingly.

2.2.3 RESOURCE REQUIREMENTS

11. The Board notes that requirement 3.1.1.2 seems repetitive and unclear, not helped by the different terminology. For example, the third paragraph reads as if the engagement partner makes the decision of suitability on their judgement alone. The Board recommends LU SA to redraft to make the requirement clearer and more understandable, using consistent terminology.

2.2.4 PROCESS REQUIREMENTS

12. The Board observes that requirement 4.2.1 provides several examples of necessary information. Nonetheless, the first two examples provided should be a requirement by themselves, in accordance with section 7.2 of the Annex 1 to the Guidelines. Therefore, the Board encourages the LU SA to amend the wording and include the above-mentioned examples as requirements.
13. With regard to section 4.4 (Evaluation) of the LU SA accreditation requirements, the Board is of the opinion that the accreditation requirements should include the obligation of the certification body to ensure that there are evaluation methods in place, and that those evaluation methods, described in the certification mechanism, are standardised and generally applicable. This would ensure that comparable evaluation methods are used for comparable targets of evaluation. Any deviations from these evaluation methods would need to be justified by the certification body. Hence, the Board recommends the LU SA to amend the draft in order to include the above-mentioned obligation for the certification body.
14. Furthermore, the Board takes note that requirement 4.4.2 states that, even though outsourcing is not allowed, the certification body can use external experts for specific areas. In this regard, it is important to clarify that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the LU SA to amend the wording in requirement 4.4.2 accordingly.
15. The Board observes that section 4.7 of the LU SA accreditation requirements ("certification documentation") does not address the requirement in the Annex for documenting the period of surveillance (section 7.9). Therefore, the Board encourages the LU SA to include the period of monitoring within the meaning of section 7.9 on surveillance.
16. With regard to section 4.8 ("directory of certified processing activities") of the LU SA accreditation requirements, requirement 4.8.1 states that the information will be provided to the public "upon request". The Board is of the opinion that, the transparency obligation set out in section 7.8 of Annex

1 would be better fulfilled if the information was made available pro-actively by the certification body. Thus, the Board recommends the LU SA to amend the draft in order to provide that the certification body will make publicly available the information referred to in section 7.8 of Annex 1 of the Guidelines.

17. The Board notes that section 4.8 has a heading for surveillance without any requirements. The Board recommends that LU SA to clarify how monitoring will be carried out.
18. Concerning the termination, reduction, suspension or withdrawal of certification (subsection 4.10), the Board notes that there is no reference to the obligation of the certification body to accept decisions and orders from the competent supervisory authority to withdraw or not to issue certification to a customer (applicant) if the requirements for certification are not or no longer met. This obligation is set out in Article 58(2)(h) GDPR as well as in section 7.11 of Annex 1. Therefore, the Board recommends the LU SA to amend the accreditation requirements specifying the rules covering withdrawal, termination, reduction or suspension of the certification .
19. The Board notes that section 9 of the annex which has general headings do not have requirements. For example, section 9.3.4 on suspension or withdrawal of accreditation is not covered here. These are significant headings that warrant cross references to the relevant sections or requirements being added. The Board encourages LU SA to clarify where the requirements are covered.

3 CONCLUSIONS / RECOMMENDATIONS

20. The draft accreditation requirements of the Luxembourg Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
 21. As general remarks, the Board recommends that the LU SA:
 1. clarifies the meaning of “standard”, as referred in several requirements (e.g. 3.2.1.1 and 4.1.2). This could be done, for example, in the “scope” or “terms and definitions” sections.
 22. Regarding ‘general requirements for accreditation’ the Board recommends that the LU SA:
 1. clarifies that the requirements cannot be overridden by any external standard, such as ISAE 3000.
 2. amends the requirements in 1.6 in order to include the obligation of the certification body to publish and make easily publicly available all versions of the approved criteria and all certification procedures, in line with the Annex to the Guidelines.
 23. Regarding ‘resource requirements’ the Board recommends that the LU SA:
 1. redrafts requirement 3.1.1.2 to make it clearer and more understandable, using consistent terminology.
 24. Regarding ‘process requirements’ the Board recommends that the LU SA:
 1. amends section 4.4 of the draft requirements in order to include the obligation of the certification body to ensure that there are evaluation methods in place, and that those

evaluation methods, described in the certification mechanism, are standardised and generally applicable. Any deviations from the evaluation methods would need to be justified by the certification body.

2. amends the wording in requirement 4.4.2 in order to make explicit that the certification body will retain the responsibility for the decision-making, even when it uses external experts.
3. amends section 4.8 of its draft accreditation requirements in order to provide that the certification body will make publicly available the information referred to in section 7.8 of Annex 1 of the Guidelines.
4. clarifies in section 4.8 how the monitoring will be carried out..
5. amends subsection 4.10 in order to specify rules covering withdrawal, termination, reduction or suspension of the certification.

4 FINAL REMARKS

25. This opinion is addressed to the LU SA and will be made public pursuant to Article 64 (5b) GDPR.
26. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 6/2020 on the draft decision of the Spanish
Supervisory Authority regarding the Controller Binding
Corporate Rules of Fujikura Automotive Europe Group (FAE
Group)**

Adopted on 29 January 2020

Table of contents

1	SUMMARY OF THE FACTS	4
2	ASSESSMENT	4
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS	5

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (EEA) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018, as last amended on 2 December 2019,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the EDPB) is to ensure the consistent application of the GDPR throughout the European Economic Area. To this effect, it follows from article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (SA) aims to approve binding corporate rules (BCRs) within the meaning of article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under the Directive 95/46/EC the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of article 47 GDPR and, in addition, conferred to the EDPB the task to issue an opinion on the competent supervisory authority’s (BCR Lead) draft decision aiming to approve BCRs. This task of EDPB aims to ensure the consistent application of the GDPR, including by the supervisory authorities, controllers and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (article 47(2) GDPR). The BCRs are subject to approval from the competent supervisory authority (“competent SA”), in accordance with the consistency mechanism set out in article 63 and 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) WP256 rev.01 of the Article 29 Working Party,³ as endorsed by the EDPB, provides for the required elements for BCRs for controllers, including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance to the supervisory authorities' national laws. The EDPB is subject to Regulation 1049/2001 pursuant to article 76(2) GDPR.

(5) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2), each application should be addressed individually and is without prejudice to the assessment of any other Binding Corporate Rules. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake and the policies and procedures that they have in place to protect personal data.⁴

(6) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft Controller BCRs of Fujikura Automotive Europe Group were reviewed by the Spanish Data Protection Authority (hereinafter Spanish Supervisory Authority) as the BCRs Lead SA.
2. The Spanish Supervisory Authority has submitted its draft decision regarding the draft Controller BCRs of Fujikura Automotive Europe Group, requesting an opinion of the EDPB pursuant to article 64(1)(f) GDPR on 10/01/2020. The decision on the completeness of the file was taken on 14/01/2020.

2 ASSESSMENT

3. The Fujikura Automotive Europe Group (FAE Group, i.e. Fujikura Automotive Europe, S.A.U. and each of its subsidiaries) draft Controller BCRs will apply to intra-group data processing and transfers and

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

specifically protect any personal data processed by FAE Group within and transferred outside of the EEA. Concerned data subjects include current and past employees, job applicants, clients, suppliers and contact persons.

4. The FAE Group draft Controller BCRs have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the FAE Group draft Controller BCRs contain all elements required under article 47 GDPR and WP256 rev01, in concordance with the draft decision of the Spanish Supervisory Authority submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns which need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

5. Taking into account the above and the commitments that the group members will undertake by signing FAE Group Intra-Group Agreement on Binding Corporate Rules, the EDPB considers that the draft decision of the Spanish Supervisory Authority may be adopted as it is, since those Rules contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within article 47(2)(k) GDPR and WP 256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

6. This opinion is addressed to the Spanish Supervisory Authority and will be made public pursuant to article 64(5)(b) GDPR.
7. According to Article 64(7) and (8) GDPR, the Spanish Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
8. Pursuant to article 70(1)(y) GDPR, the Spanish Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 7/2020 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR)

Adopted on 22 April 2020

Table of contents

1	SUMMARY OF THE FACTS	5
2	ASSESSMENT.....	5
2.1	General reasoning of the EDPB regarding the additions in the submitted list.....	5
2.2	Application of the consistency mechanism to the draft list.....	6
2.3	Analysis of the draft list.....	6
	Management of commercial activities.....	6
3	CONCLUSIONS / RECOMMENDATIONS.....	6
4	FINAL REMARKS	6

The European Data Protection Board

Having regard to Article 63, Article 64(2), Article 64(3) and Article 35(1), (5), (6) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to Article 51(1)(b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 10 and 22 of its Rules of Procedure,

Having regard to Opinion 13/2019 on the draft list of the competent supervisory authority of France regarding the processing operations exempt from the requirement of a data protection impact assessment (Article 35(5) GDPR) by the EDPB

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereinafter GDPR) throughout the European Economic Area. In compliance with Articles 35(6) and 64(2) GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to adopt a list of processing operations not subject to the requirement for a data protection impact assessment pursuant to Article 35(5) GDPR. The aim of this opinion is therefore to create a harmonised approach with regard to processing that is cross border or that can affect the free flow of personal data or natural person across the European Union. Even though the GDPR doesn't impose a single list, it does promote consistency. The Board seeks to achieve this objective in its opinions by ensuring that the lists do not contradict the cases where the GDPR explicitly states that a type of processing should undergo a data protection impact assessment (hereinafter "DPIA"), by recommending SAs to remove some criteria which, the Board considers not correlated with the absence of likelihood of high risks for data subjects, by recommending them to limit the scope of the types of processing in order not to contradict the general rules defined in the DPIA guidelines of the Article 29 Working Party², endorsed by the EDPB, and finally by recommending them to use some criteria in a harmonized manner.

(2) With reference to Article 35(5) and (6) GDPR, the competent supervisory authorities may establish lists of the kind of processing operations which are not subject to the requirement for a DPIA. They shall, however, apply the consistency mechanism where such lists involve processing operations, which are related to the offering of goods or services to data subjects or to the monitoring of their

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² WP29 - 248 rev.1, 4 April 2017, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679- endorsed by the EDPB.

behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

(3) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. Pursuant to Article 64(3) GDPR, the EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) While the draft lists of the competent supervisory authorities are subject to the consistency mechanism, this does not mean that the lists should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB assessment/opinion is not to reach a single EU list but rather to avoid significant inconsistencies that may affect the equivalent protection of the data subjects across the EEA.

(5) The carrying out of a DPIA is only mandatory for the controller pursuant to Article 35(1) GDPR where processing is “likely to result in a high risk to the rights and freedoms of natural persons”. The national SAs can issue lists concerning certain processing activities, which always require a DPIA (blacklists) per Article 35(4) as well as lists where no DPIA is necessary per Article 35(5) (whitelists). When a processing does not fall within either of these two lists and is not mentioned by Article 35(3) GDPR, an ad hoc decision will have to be made by the data controller based on whether the “likely to result in a high risk to the rights and freedoms of natural persons” criterion is met. According to Recital 91 of the GDPR, a DPIA will not be mandatory when the processing is carried out by an individual physician, other health care professional or a lawyer, as it is not of a sufficient large scale. This exception covers only partially the cases when a DPIA will not be necessary, i.e. when there is no high risk to the rights and freedoms of natural persons.

(6) The lists produced by the competent supervisory authorities support a common objective, namely to identify the kind of processing operations for which the national SAs are certain that, under no circumstances, they will result in a high risk, and processing operations the national SAs deem unlikely to result in a high risk, and therefore do not require a DPIA. The Board refers to the DPIA guidelines of the Article 29 Working Party, which sets out criteria to consider in determining processing operations “*likely to result in a high risk*”.³ As set out in these guidelines, in most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. However, in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA.

(7) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

³ Recitals 75, 76, 92, 116 GDPR.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The competent supervisory authority of France has submitted its draft list to the EDPB, which contains two additions to their previously adopted list. The decision on the completeness of the file was taken and the request circulated on 26 February 2020.
2. The opinion must be adopted on 22 April 2020.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the additions in the submitted list

3. Any list submitted to the EDPB has been interpreted as further specifying on the one hand Article 35 GDPR, which will prevail in any case, and on the other hand recital 91. Thus, no list can be exhaustive.
4. This opinion does not reflect upon items submitted by the French Supervisory Authority, which were deemed outside the scope of Article 35(6) GDPR. This refers to items that neither relate "to the offering of goods or services to data subjects" in several Member States nor to the monitoring of the behaviour of data subjects in several Member States. Additionally, they are not likely to "substantially affect the free movement of personal data within the Union". However, for the sake of clarity, the Board will enumerate the items of the list, which were deemed outside the scope of Article 35(6) GDPR. Further, any processing operations that relate to law enforcement were deemed out of scope, as they are not in scope of the GDPR.
5. This opinion will not comment on any items on the list, which fall within the scope of recital 91.
6. The opinions on the Article 35(4) GDPR lists also aimed at defining a consistent core of processing operations, which the Board requested all Supervisory Authorities to add to their list if not already present in order to ensure consistency. The Article 35(5) GDPR lists may not exempt these general processing operations as a rule.
7. The lists established by SAs pursuant to Article 35(5) GDPR are inherently non-exhaustive. These lists contain types of processing regarding which national SAs are certain that, under no circumstances, they will result in a high risk to the rights and freedom of natural persons, and processing operations the national SAs deem unlikely to result in a high risk. Such lists cannot enumerate all cases in which a DPIA will not be necessary. In any event, the obligation of the controller or processor to assess the risk of the processing and to comply with the other obligations imposed by the GDPR remain applicable.
8. When this opinion remains silent on an item from the list, it means that the Board is not asking the French Supervisory Authority to take further action.
9. Finally, the Board recalls that transparency is key for data controllers and data processors. In order to clarify the entries in the list, the Board is of the opinion that making an explicit reference in the lists to the criteria set out in the guidelines could improve this transparency.

2.2 Application of the consistency mechanism to the draft list

10. The draft list submitted by the French Supervisory Authority relates to the offering of goods or services to data subjects, relates to the monitoring of their behaviour in several Member States and/or may substantially affect the free movement of personal data within the Union mainly because the processing operations in the submitted draft list are not limited to data subjects in this country.
11. The EDPB notes that for the items 13 and 14 that each mentioned “frame of reference” document is deemed to be part of the draft decision.
12. Further, the EDPB has previously considered the items 1-12 of the submitted draft decision in the context of its Opinion 13/2019.
13. Regarding item 13 and considering Article 64(3) GDPR, the Board recalls that in its Opinion 13/2019 to the FR SA it stated that for these kinds of processing the scope needs to be restricted by “stating that it does not apply to the processing activities concerning debts which have been acquired from a third party, and that it only applies to debts owed in the context of a business to consumer relationship. Furthermore, the Board recommends that evaluation and scoring be explicitly excluded from scope of this item.”

2.3 Analysis of the draft list

14. Taking into account that:
 - a. Article 35(1) GDPR requires a DPIA when the processing activity is likely to result in a high risk to the rights and freedoms of natural persons; that
 - b. Article 35(3) GDPR provides a non-exhaustive list of types of processing that require a DPIA, and that
 - c. the Board presently only considers the item 14 of the submitted draft decision, the Board is of the opinion that:

MANAGEMENT OF COMMERCIAL ACTIVITIES

15. The Board recalls its reasoning in its Opinion 11/2019 where it requested for these kind of processing activities the restriction of “the scope of this item by covering only business-to-customers relations, excluding the processing of sensitive data or data of highly personal nature and by excluding data processing on a large scale.” The Board therefore recommends that the FR SA reduces the scope of this item in the same way.

3 CONCLUSIONS / RECOMMENDATIONS

16. The draft list of the French Supervisory Authority may lead to an inconsistent application of Article 35 GDPR and recommends that the following changes be made:
 - ✓ Regarding management of commercial activities: the Board recommends to restrict the scope of this item by covering only business-to-customers relations and the exclusion of the processing of sensitive data or data of highly personal nature from the item.

4 FINAL REMARKS

17. This opinion is addressed to the Commission Nationale de l’Informatique et des Libertés (French Supervisory Authority) and will be made public pursuant to Article 64(5)(b) GDPR.

18. The French Supervisory Authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 9/2020 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of Reinsurance Group of America

Adopted on 14 April 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (EEA) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the EDPB) is to ensure the consistent application of the GDPR throughout the European Economic Area. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (SA) aims to approve binding corporate rules (BCRs) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under the Directive 95/46/EC the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR and, in addition, conferred to the EDPB the task to issue an opinion on the competent supervisory authority’s (BCR Lead) draft decision aiming to approve BCRs. This task of EDPB aims to ensure the consistent application of the GDPR, including by the supervisory authorities, controllers and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent supervisory authority (“competent SA”), in accordance with the consistency mechanism set out in Article 63 and 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party¹, endorsed by the EDPB.

¹ The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) WP257 rev.01 of the Article 29 Working Party,² as endorsed by the EDPB, provides for the required elements for BCRs for processors, including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of article 47 GDPR and WP257 rev01. The EDPB is subject to Regulation 1049/2001 pursuant to article 76(2) GDPR.

(5) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2), each application should be addressed individually and is without prejudice to the assessment of any other Binding Corporate Rules. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake and the policies and procedures that they have in place to protect personal data.³

(6) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft Processor BCRs of Reinsurance Group of America were reviewed by the Irish Data Protection Commission (hereinafter Irish Supervisory Authority) as the BCRs Lead SA.
2. The Irish Supervisory Authority has submitted its draft decision regarding the draft Processor BCRs of Reinsurance Group of America, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 18/02/2020. The decision on the completeness of the file was taken on 26/03/2020.

2 ASSESSMENT

3. The EDPB notes that the Reinsurance Group of America has only provided one Intra Group Agreement (IGA), common to both the Controller BCR and Processor BCR. Since Reinsurance Group of America has provided two different sets of BCRs and Annexes, and the IGA makes a clear distinction in its relevant provisions, the EDPB considers that no further documents need to be submitted in this regard.
4. The Reinsurance Group of America draft Processor BCRs apply to processing of personal data carried out, within the group, by members of the Group acting as a Processor on behalf of and under the instructions of a non-RGA Controller and where such personal data originates in the EEA. Concerned

² Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

³ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

data subjects include individuals who are parties to or beneficiaries of primary individual or group insurance and pension policies, as well as current and past employees, job applicants, individual consultants, independent contractors and job applicants that RGA may process on behalf of the Controller.

5. The Reinsurance Group of America draft Processor BCRs have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Reinsurance Group of America draft Processor BCRs contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the Irish Supervisory Authority submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns, which need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Reinsurance Group of America's Intra-Group Agreement on Binding Corporate Rules, the EDPB considers that the draft decision of the Irish Supervisory Authority may be adopted as it is, since those Rules ensure appropriate safeguards to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Irish Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Irish Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Irish Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 10/2020 on the draft decision of the competent supervisory authorities of Germany regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 25 May 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the DE SAs' draft accreditation requirements for Code of Conduct's monitoring bodies ...	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	6
2.2.3	CONFLICT OF INTEREST	6
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES.....	7
2.2.5	TRANSPARENT COMPLAINT HANDLING.....	7
3	CONCLUSIONS / RECOMMENDATIONS	7
4	FINAL REMARKS.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes of conduct. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The German Supervisory Authorities of the Federation and the Länder (hereinafter "DE SAs") have submitted their draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c) GDPR, for a consistent approach at Union level. The decision on the completeness of the file was taken on 13 February 2020.
2. In compliance with article 10 (2) of the Board's Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board's opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly requests SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (Article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the DE SAs to take further action.
8. This opinion does not reflect upon items submitted by the DE SAs, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the DE SAs' draft accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. For the sake of consistency, the Board encourages the DE SAs to use the Guidelines terminology in the draft accreditation requirements and replace the word “criteria” by the word “requirements” in the title of the draft accreditation requirements.
11. The Board notes that in the introductory part under section 3 of the DE SAs' draft accreditation requirements, which defines the powers of the monitoring body, it is stated that the relationship between the monitoring body and the code members is subject to regulation by private law agreement. The Board highlights that the binding nature of the rules of the code of conduct, including those providing for the monitoring mechanism, would result from the (mere) adhesion of the code members to the code, as well as from their membership of the representative association. Whereas contractual arrangements are not, *per se*, excluded, the Board is of the opinion that the essential elements of the monitoring body's function should be included in the code itself. Additional clauses

may be added in the form of an agreement or contract between the monitoring body and the code member, as long as they do not entail a variation in the essential elements of the monitoring body's function, as set out in the code. Therefore, the Board recommends the DE SAs to specify that the core elements of the monitoring body's function will be included in the code of conduct.

2.2.2 INDEPENDENCE

12. The Board observes that the draft accreditation requirements do not make an explicit reference to "accountability" as one of the four areas in which the monitoring body shall demonstrate independence. The Board considers that the independence of the monitoring body shall be demonstrated in four areas: 1) Legal and decision making procedures, 2) financial, 3) organisational and 4) accountability.² Therefore, the Board recommends that the DE SAs include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.
13. The Board observes that the introductory paragraph under section 2.2 of the DE SAs' draft accreditation requirements refers to independence of the monitoring body in relation to the "sectoral subject matter of the code of conduct". The Guidelines (paragraph 63) provide further information on how independence of the monitoring body can be demonstrated, for example by demonstrating independence in relation to the profession, industry or sector to which the code applies. Therefore, the Board encourages the DE SAs to redraft this part of the requirements in line with the Guidelines by stating, for example, that the profession, industry or sector to which the code applies are included within the "sectoral subject matter".
14. With regard to section 2.2.1 of the DE SAs' draft accreditation requirements, the Board takes note of all the elements demonstrating the monitoring body's independence with respect to its organisational structure. Among others, it is stated that the monitoring body cannot be penalised for the performance of its tasks. The Board considers that it should be further clarified that the monitoring body assumes responsibility for its activities, and it cannot be penalised by neither the code owner nor the code members. Therefore, the Board encourages the DE SA to redraft this part of the requirement so that the monitoring body is protected against any dismissal or sanction, direct or indirect, for the performance of its duties.
15. The Board notes the requirement for the monitoring body to demonstrate adequate financial resources in order to cover liability claims, among others (section 2.2.2 of the DE SAs' draft accreditation requirements). However, the Board is of the opinion that such a requirement might appear disproportionately burdensome for small and medium enterprises that might be discouraged from applying for accreditation. In this regard, the Board recommends that the DE SAs soften the wording of this section, referring to the monitoring body's responsibilities in a general manner.

2.2.3 CONFLICT OF INTEREST

16. Regarding the individual activities and processes of the monitoring activity that can be outsourced to external service providers (section 2.5 of the DE SAs' draft accreditation requirements), the Board considers that the fact that the obligations applicable to the monitoring body are also applicable to the subcontractors should be clearly stated in the requirements. For this reason, the Board recommends the DE SAs to add the words "and obligations" after the word "requirements" and delete the word "essentially" from the first bullet point under section 2.5.

² The EDPB developed these areas in more detail in the Opinion 9/2019 on the Austrian SA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

17. Section 2.6.1.2 of the DE SAs' draft accreditation requirements states that the monitoring body will assess whether code members are able to implement the codes of conduct by carrying out a "representative random sampling". According to Article 41 (2)(b) GDPR and paragraphs 70 and 71 of the Guidelines, the monitoring body will need to have appropriate governance structures and procedures, which allow for it to adequately assess the eligibility of controllers and processors to sign up and comply with the code. The Board questions how assessment based on representative random sampling could satisfy the requirements set out in paragraph 71 of the Guidelines, which ask that "*comprehensive vetting procedures*" should be in place in order to "*adequately assess the eligibility of controllers and processors to sign up and comply with the code*". Therefore, the Board recommends that the DE SA deletes reference to "representative random sampling".
18. Section 2.6.1.3 of the DE SAs' draft accreditation requirements, which refers to the verification of the application and monitoring of compliance with the code of conduct, seems reduce the possible monitoring procedures. Depending on the context of the code of conduct, the Board considers that a larger variety of monitoring procedures could also lead to an efficient verification of the application and monitoring of compliance with the code of conduct. For this reason, the Board encourages the DE SAs to redraft this section. For example, references to ad hoc inspections in case of complaints against a particular code member or on site visits to assess compliance with the code could be included, in line with paragraph 72 of the Guidelines.
19. The Board notes that, with regard to the design of the relevant code of conduct, additional tasks may arise for the monitoring bodies of the respective code of conduct (section 2.6.1.5 of the DE SAs' draft accreditation requirements). The Board acknowledges that, but encourages the DE SA to ensure that these additional tasks will not impair the effectiveness and impartiality of the monitoring body's monitoring activities.

2.2.5 TRANSPARENT COMPLAINT HANDLING

20. The Board notes that section 4.2 of the DE SAs' draft accreditation requirements states that publication of the complaints should be carried out both by the monitoring body and the code members. Similar considerations can be made with regards to section 3.1 of the draft accreditation requirements devoted to the code members' obligations to provide the monitoring body with the contact details and contact persons of code members. The Board encourages the DE SAs not to include obligations imposed on code members in the requirements for monitoring bodies and redraft these sections accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

21. The draft accreditation requirements of the German Supervisory Authorities of the Federation and the Länder may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
 22. Regarding *general remarks* the Board recommends that the DE SAs:
 1. specify, in section 3, that the core elements of the monitoring body's function will be included in the code of conduct.
 23. Regarding *independence* the Board recommends that the DE SAs:

1. include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.
 2. redraft section 2.2.2 describing the monitoring body's responsibilities in a general manner, with regards to the adequacy of its financial resources.
24. Regarding *conflict of interest* the Board recommends that the DE SAs:
1. add the words "and obligations" after the word "requirements" and deletes the word "essentially" from the first bullet point under section 2.5.
25. Regarding established procedures and structures the Board recommends that the DE SAs:
1. delete the reference to "representative random sampling" from section 2.6.1.2.

4 FINAL REMARKS

26. This opinion is addressed to the German supervisory authorities of the Federation and the Länder and will be made public pursuant to Article 64 (5) (b) GDPR.
27. According to Article 64 (7) and (8) GDPR, the DE SAs shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether they will amend or maintain their draft decision. Within the same period, they shall provide the amended draft decision or where they do not intend to follow the opinion of the Board, they shall provide the relevant grounds for which they do not intend to follow this opinion, in whole or in part.
28. The DE SAs shall communicate the final decision to the Board for inclusion in the register of decisions that have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 11/2020 on the draft decision of the competent supervisory authority of Ireland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 25 May 2020

Table of contents

1	Summary of the facts	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the IE accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	6
2.2.3	CONFLICT OF INTEREST	7
2.2.4	EXPERTISE.....	7
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	8
2.2.6	TRANSPARENT COMPLAINT HANDLING.....	8
2.2.7	COMMUNICATING WITH THE IE SA	8
2.2.8	CODE REVIEW MECHANISMS.....	8
2.2.9	LEGAL STATUS	9
3	CONCLUSIONS / RECOMMENDATIONS.....	9
4	FINAL REMARKS	10

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41 GDPR. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt these requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term ‘accreditation’. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and demonstrate how

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Irish Supervisory Authority (hereinafter "IE SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 13 February 2020.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements
3. All accreditation requirements submitted to the Board for an opinion must fully address article 41(2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1)(p) GDPR, all the SAs should cover these basic core requirements

Adopted

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to 'encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking into account the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises' (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the IE SA to take further action.
8. This opinion does not reflect upon items submitted by the IE SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the IE accreditation requirements for Code of Conduct's monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct,

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The Board supports the development of voluntary compliance activities, including the drawing up of Codes aimed to contribute to the proper application of the GDPR by different sectors of different sizes, and covering processing activities with different levels of risk. In this context, the Board supports the emphasis made by IE SA on the specific needs of micro, small and medium sized enterprises.
11. The Board notes that IE SA introduced a number of examples that in overall help in the interpretation of the draft decision. However, some of the examples are better suited as a requirement, rather than as an example. Therefore, the Board recommends the IE SA to revise the draft accordingly.
12. The Board encourages the IE SA to include in the draft accreditation requirements some examples of the information or documents that applicants have to submit when applying for accreditation.

Adopted

2.2.2 INDEPENDENCE

13. The Board considers that there are four areas where the monitoring body should demonstrate its independence: 1) legal and decision-making procedures; 2) financial; 3) organisational; 4) accountability.² With regards to the IE SA requirements, it seems that the first and the third areas are covered by section 1.1, devoted to ‘Structure, Power, and Functions’ and the second area is covered by Section 1.2 headed ‘Budget and Resources’. However, the Board notices that there is no reference to the fourth area related to accountability.
14. In this regard, the Board notes that the monitoring body should be able to demonstrate “accountability” for its decisions and actions in order to be considered to be independent. The IE SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate its accountability. This could be accomplished through such things as setting out the roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the personnel about the governance structures and the procedures in place. Thus, the Board recommends the IE SA to introduce the above-mentioned requirements related to accountability of the monitoring body.
15. Regarding section 1.1.2 of the IE SA’s draft accreditation requirements, which addresses the issue of internal monitoring body, the Board is of the opinion that independence should exist not only towards the larger entity but with respect to the overall group structure. According to the point 65 of the Guidelines, where an internal monitoring body is proposed, there should be separate personnel and management, accountability and function from other areas of the organisation. This may be achieved in a number of ways, for example, by the use of effective organisational and information barriers and separate reporting management structures for the association and monitoring body. The monitoring body should be able to act free from instructions and shall be protected from any sort of sanctions or interference as a consequence of the fulfilment of its task. In this context, the Board encourages the IE SA to better explain this section and clarify that independence needs to be ensured towards the larger entity, in particular the code owner.
16. As regards section 1.2.1 of the IE SA’s draft accreditation requirements, the Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. Therefore, the Board recommends that the IE SA amend the explanatory note, adding a reference to such procedures.
17. The Board underlines that the code owners should be able to demonstrate that the proposed monitoring body have adequate resources and personnel to carry out its tasks in an appropriate manner. In particular, resources should be proportionate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing (see paragraph 73 of the Guidelines). The Board notes that in this context, section 1.2.4 of the IE SA’s draft requirements lacks some criteria that should be used to measure the adequacy of monitoring body’s resources and personnel. Therefore, the Board encourages the IE SA to add some additional details in the draft requirements, such as the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing.

² The EDPB developed these areas in more detail in the Opinion 9/2019 on the Austrian SA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR.

18. With regard to the use of sub-contractors, the Board notes that section 1.2.5 of the IE SA's draft accreditation requirements state that "the use of subcontractors does not remove the responsibility of the monitoring body". Indeed, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the IE SA to specify that, notwithstanding the sub-contractor's responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance. In addition, the Board is of the opinion that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. The Board recommends the IE SA to explicitly add this obligation in the draft accreditation requirements.

2.2.3 CONFLICT OF INTEREST

19. The Board recognizes that one of the biggest risks related to the monitoring body is the risk of impartiality. The Board notes that such a risk may arise not only from providing services to the code members but also from a wide range of activities carried out by the monitoring body vis-à-vis code owners (especially in the situation where the monitoring body is an internal one) or other relevant bodies of the sector concerned. In this context, the Board encourages the IE SA to reword the requirement in point 2.1 in more general terms and provide additional clarifications and examples of situations where there is no conflict of interest. Examples could include, among others, services, which are purely administrative or organisational assistance or support activities, which have no influence on the impartiality of the monitoring body.

2.2.4 EXPERTISE

20. With respect to the explanatory note in section 3 of the IE SA's draft accreditation requirements ("Expertise"), the Board notes that, as required by the Guidelines, every code owner has to demonstrate 'why their proposals for monitoring are appropriate and operationally feasible' (see paragraph 41 of the Guidelines). In this context, all codes with monitoring bodies will need to explain the necessary expertise level for their monitoring bodies in order to deliver the code's monitoring activities effectively. To that end, in order to evaluate the expertise level required by the monitoring body, a code owner should, in general, take into account such factors as: the size of the sector concerned, the different interests involved and the risks of the processing activities addressed by the code. This would also be important if there are several monitoring bodies, as the code will help ensure a uniform application of the expertise requirements for all monitoring bodies covering the same code.
21. With respect to section 3.3 of the IE SA's draft accreditation requirements and the reference to "operational experience, training, and qualifications", in line with the Guidelines (paragraph 69), the Board encourages IE SA to clarify which type of operational experience is required in the text of the requirement itself (i.e. experience in monitoring of compliance, such as in the field of auditing, monitoring, or quality assurance activities).
22. As regards section 3.4 of the IE SA's draft accreditation requirements, the Board considers that it should be better coordinated with sections 3.1, 3.2 and section 3.3, in order to avoid confusion with regard to the scope of section 3.4 in connection with the previous three. Therefore, the Board encourages the IE SA to clarify the relationship between those sections specifying that the monitoring body will have to meet the expertise requirements in sections 3.1, 3.2 and 3.2 in any circumstances, whereas further or specific expertise requirements will only need to be met in case that the code of conduct foresees them.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

23. The Board observes that sections 4.2 and 4.3 of the IE SA's draft accreditation requirements refer to the complexity and risks involved, as part of the criteria to be taken into account in the assessment of the established procedures to monitor compliance of code members with the Code and for the periodic review of the operations of the code, respectively. For the sake of clarity, the Board encourages the IE SA to specify that the complexity and the risks refer to the sector concerned and the data processing activities to which the code applies.
24. With respect to sections from 4.2 to 4.5 of the IE SA's draft accreditation requirements, the Board considers some clarity could be provided with regard to periodic review. This, as well as the meaning of "periodically" and "ad hoc" could be clarified in the explanatory note, in particular by providing examples.

2.2.6 TRANSPARENT COMPLAINT HANDLING

25. With respect to the explanatory note introduced at the beginning of section 5 of the IE SA's draft accreditation requirements ("Transparent Complaint Handling") and its last sentence, the Board is of the opinion that it should be specified what are the 'monitoring body's other monitoring activities'. Therefore, the Board encourages the IE SA to clarify that this term refers to the monitoring activities other than formal decisions.

2.2.7 COMMUNICATING WITH THE IE SA

26. According to the explanatory note provided in section 6 of the IE SA'S draft accreditation requirements, 'a proposed framework for any monitoring body needs to allow for the effective communication of *any actions* carried out by the monitoring body in respect of monitoring of compliance with the Code to the DPC'. In this context, the Board is of the opinion that it should be clarified that not every single action carried out by the monitoring body shall be communicated to the IE SA. The Board underlines that communicating of every single action may create a risk of overloading the IE SA with an excessive amount of information. The same comment applies to section 6.2 and the mention of the "outcome of any audit, review or investigation of a code member's compliance with the code" as well as to section 6.3 and the reference to "procedure for notifying the DPC of any complaints made against it". Therefore, the Board encourages the IE SA to amend the draft accordingly and specify that in general not all the complaints and not every single action, audit, review or investigation vis-à-vis code members is communicated to IE SA.
27. Still with regard to section 6.2 of the IE SA's draft accreditation requirements, the example provided seems to imply that the documentation regarding "any audit, review or investigation of a code member's compliance with the code" or "any review of previously exercised exclusions or suspension from the code" will be made available to the IE SA upon request. However, from the text of the requirement itself, it is unclear whether the notification to the IE SA will take place at the monitoring body's initiative (i.e. irrespective of any request by the SA) or at the request of the IE SA. Therefore, the Board encourages the IE SA to amend the example in order to clarify this issue.

2.2.8 CODE REVIEW MECHANISMS

28. The Board notes that section 7.3 of the draft requirements states that the monitoring body will apply and implement updates, amendments and/or extensions to the Code. Since the updating of the code of conduct is responsibility of the code owner, the Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. As an example, section 7.3 of the IE's draft

accreditation requirements could be amended as follows: “The monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner”. The Board encourages the IE SA to amend the draft accordingly.

2.2.9 LEGAL STATUS

29. As regards section 8 of the IE SA’s draft accreditation requirements, the Board notes that in the draft accreditation requirements there is no provision that would explicitly state that the monitoring body must be located within the European Economic Area. The Board is of the opinion that monitoring bodies require an establishment in the EEA. This is to ensure that they can fully uphold data subject rights, deal with complaints and be effectively supervised by the competent SA, so that to guarantee the enforceability of the GDPR. The Board recommends that the IE SA require that the monitoring body has an establishment in the EEA.
30. According to requirement 8.2 of the IE SA’s draft accreditation requirements, the monitoring body shall have financial resources to ensure that fines per Article 83(4)(c) GDPR can be imposed on the monitoring body and met. In the Board’s opinion, financial capacity shall not prevent small or medium monitoring bodies from being accredited. It is enough to have a legal capability of being fined. Therefore, the Board encourages the IE SA to either delete this requirement or to soften the wording and refer to the monitoring body’s responsibilities in general. Moreover, the third paragraph of the example as provided in section 8.3 of the draft requirements should be amended accordingly, and the Board encourages the IE SA to do so.
31. At the same time, the Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. Therefore, the Board encourages that the IE SA amend the explanatory note, adding in it a reference to long-term financing.

3 CONCLUSIONS / RECOMMENDATIONS

32. The draft accreditation requirements of the Irish Supervisory Authority create a risk of an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
33. As general remarks, the Board recommends that the IE SA:
 1. amend the draft to make a clear distinction between examples and requirements.
34. Regarding ‘independence’ the Board recommends that the IE SA:
 1. include a reference to the accountability of the monitoring body;
 2. in section 1.2.1 include a reference to the procedures that ensure the functioning of the code of conduct over time;
 3. in section 1.2.5 include obligation on monitoring body to ensure effective monitoring of the services provided by its sub-contractors.
35. Regarding ‘legal status’ the Board recommends that the IE SA:
 1. require in section 8 that the monitoring body has an establishment in the EEA.

Adopted

4 FINAL REMARKS

36. This opinion is addressed to the Irish supervisory authority and will be made public pursuant to Article 64 (5)(b) GDPR.
37. According to Article 64 (7) and (8) GDPR, the IE SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
38. The IE SA shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



Opinion 13/2020 on the draft decision of the competent supervisory authority of Italy regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 25 May 2020

Table of contents

1	SUMMARY OF THE FACTS	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the IT accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE	5
2.2.3	CONFLICT OF INTEREST	7
3	CONCLUSIONS / RECOMMENDATIONS.....	7
4	FINAL REMARKS	7

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018, as last modified and adopted on 10 September 2019

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Italian Supervisory Authority (hereinafter "IT SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 13 February 2019.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (Article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the IT SA to take further action.
8. This opinion does not reflect upon items submitted by the IT SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the IT accreditation requirements for Code of Conduct’s monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. For the sake of consistency and clarity, the EDPB encourages the IT SA to replace throughout the draft accreditation requirements the terms “association/ organisation owning the CoC” and “association/ organisation submitting the CoC” with the term “Code owner” in line with the terminology used in the Guidelines.

2.2.2 INDEPENDENCE

11. The Board observes that, in section 3 of the IT SA’s draft accreditation requirements (“autonomy, independence, impartiality”), it is mentioned that *“accreditation shall be granted if autonomy, independence and impartiality of the monitoring body as required to fulfil the respective monitoring*

obligations are demonstrated (...)". The Board encourages the IT SA to delete reference to autonomy, for the sake of clarity and consistency.

12. For the sake of clarity, the Board encourages the IT SA to clarify the meaning of "membership of the monitoring body" and "term of the monitoring body" under section 3a ("legal status and decision-making process"), first paragraph of the draft accreditation requirements
13. Furthermore, the Board is of the opinion that internal monitoring bodies cannot be set up within a code member, but only within a code owner. Therefore, the Board recommends that this is clarified and reflected in the text of the draft accreditation requirements in the second paragraph of section 3a.
14. With regard to the legal status and decision-making process of the IT SA's draft accreditation requirements (section 3a), the Board acknowledges the impartiality of the monitoring body from the code members, the profession, industry or sector to which the code applies. However, the Board is of the opinion that these requirements should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members. For this reason, the Board encourages the IT SA to amend this paragraph accordingly.
15. With regard to the financial independence of the IT SA's draft accreditation requirements (section 3b), the Board notes that the monitoring body shall obtain financial support for its monitoring role in a way that does not compromise its independence. However, the Board considers that further explanation is needed as to how long-term financial stability of the monitoring body is ensured. In particular, the Board recommends that the IT SA amend the requirements in order to explain how financial independence is guaranteed in case one or more funding sources are no longer available.
16. Furthermore, the Board considers that the section concerning the financial independence should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. These include the number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the processing operation(s). Therefore, the Board encourages the IT SA to redraft the requirements accordingly.
17. The Board takes note of the requirements with regard to the organisational independence, under section 3c of the draft accreditation requirements, however it considers that these requirements should be further specified. For this reason, the Board encourages the IT SA to redraft this part of the requirements by adding examples of how such independence can be achieved. For example, the organisational independence can be demonstrated with a differentiated payroll, analytical accounting systems with different responsibility centres or any other logical separation that can rise firewalls between the monitoring body and the code owners or code members.
18. The second explanatory note under section 3c of the IT SA's draft accreditation requirements ("organisational independence") refers to the use of sub-contractors by the monitoring body. The Board is of the opinion that the sub-contractors should be able to ensure the same degree of safeguards provided by the monitoring body in performing their activities, including the same level of competence and expertise. At the same time, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the IT SA to specify that, notwithstanding the sub-contractor's responsibility and obligations, the monitoring

body is always the ultimate responsible for the decision-making and for compliance. In addition, the Board is of the opinion that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. The Board recommends the IT SA to explicitly add this obligation in the draft accreditation requirements.

2.2.3 CONFLICT OF INTEREST

19. The Board takes note of all the requirements included in the IT SA's draft accreditation requirements in order for the monitoring body to demonstrate that the exercise of its tasks and duties does not result in a conflict of interest (section 4). The Board encourages the IT SA to add examples in the requirements in this respect. For example, employees of the monitoring body should be required to report possible conflicts of interest.
20. Furthermore, the Board is of the opinion that, for practical reasons, examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the IT SA to add some examples, similar to the one provided in this paragraph.

3 CONCLUSIONS / RECOMMENDATIONS

21. The draft accreditation requirements of the Italian Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
22. Regarding *independence* the Board recommends that the IT SA:
 1. clarify in the second paragraph of section 3a that internal monitoring bodies cannot be set up within a code member, but only within a code owner.
 2. explain in section 3b how financial independence is guaranteed in case one or more funding sources are no longer available.
 3. add in section 3c that even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.

4 FINAL REMARKS

23. This opinion is addressed to the Italian supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
24. According to Article 64 (7) and (8) GDPR, the IT SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
25. The IT SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 14/2020 on the draft decision of the competent supervisory authority of Ireland regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 25 May 2020

Table of contents

1	Summary of the Facts	4
2	Assessment	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX (Section 0 of the IE SA's draft accreditation requirements).....	6
2.2.2	TERMS AND DEFINITIONS	6
2.2.3	GENERAL REMARKS	6
2.2.4	GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements)	7
2.2.5	STRUCTURAL REQUIREMENTS (Section 5 of the draft accreditation requirements)	7
2.2.6	RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)	7
2.2.7	PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements).....	7
3	Conclusions / Recommendations	8
4	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex 1 to the EDPB Guidelines 4/2018 on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2) GDPR. In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 GDPR provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b) GDPR. The EDPB notes that Article 43(2)(a)-(e) GDPR reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Irish Supervisory Authority (hereinafter “IE SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 13 February 2020. The IE national accreditation body (INAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the INAB will use ISO 17065 and the additional requirements set up by the IE SA, once they are approved by the IE SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the IE SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

4. This assessment of IE SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the IE SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the IE SA to take further action.
9. This opinion does not reflect upon items submitted by the IE SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- 1) addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- 2) independence of the certification body
- 3) conflicts of interests of the certification body
- 4) expertise of the certification body
- 5) appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- 6) procedures for issuing, periodic review and withdrawal of GDPR certification; and
- 7) transparent handling of complaints about infringements of the certification.

10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
 - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
 - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
 - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
 - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

[2.2.1 PREFIX \(Section 0 of the IE SA's draft accreditation requirements\)](#)

11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

[2.2.2 TERMS AND DEFINITIONS](#)

12. The Board notes that the reference to the guidelines on accreditation as "WP 261" is not updated. The EDPB adopted the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). Therefore, the Board encourages the IE SA to amend the wording and refer to the Guidelines 4/2018.

[2.2.3 GENERAL REMARKS](#)

13. The Board notes that the IE SA's draft requirements refer repeatedly to the "competent supervisory authority". Since the competent SA in this case is the IE SA, the Board encourages the IE SA to replace the reference by "the DPC" or "the IE SA" in order to avoid confusion.
14. The Board acknowledges that the IE SA's draft requirements include a section on terms and definitions. However, some of the terms are not used consistently throughout the document (e.g.

“object of evaluation” and “ToE”). In order to avoid confusion, the Board encourages the IE SA to use consistent terminology in the draft requirements.

2.2.4 GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements)

15. With regard to clause 7 of subsection 4.1.2 of the IE SA’s draft accreditation requirements, the Board considers that the wording is slightly unclear with regard to whom the reasons for approving certification are provided. Moreover, the reference to “facilitating” the register is also unclear. Therefore, the Board encourages the IE SA to redraft it in a way that provides more clarity.

2.2.5 STRUCTURAL REQUIREMENTS (Section 5 of the draft accreditation requirements)

16. The Board observes that the IE SA’s draft accreditation requirements make reference to the appointment of “a person with the relevant seniority with responsibility for overseeing data protection compliance and information governance.” The reference to the relevant seniority should be clarified in terms of experience and the scope of authority. Moreover, the functions of this figure seem similar to those of a data protection officer. The Board encourages the IE SA to clearly set out the functions of this figure and to specify the relevant experience.

2.2.6 RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)

17. Concerning certification body personnel (subsection 6.1), the Board notes that the requirements for personnel with technical expertise responsible for making decisions include having at least 5 years of professional experience related to the subject matter of certification, whereas the personnel responsible for evaluations should have at least 2 years of professional experience. Similarly, personnel with legal expertise taking decisions must have at least 5 years of professional experience, whereas those in charge of evaluations must have at least 2 years of experience. The Board notes that the required minimum years of professional experience between the personnel in charge of decision-making and the personnel in charge of evaluation differ significantly. In this regard, the Board considers that the emphasis should be put on the different type of expertise rather than on the number of years of professional experience. In the Board’s opinion, evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the IE SA to make more emphasis on the different substantive knowledge and/or experience for evaluators and decision-makers and to reduce the divergences in the years of experience required for them.

2.2.7 PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements)

18. With regard to subsection 7.10 of the IE SA’s draft accreditation requirements (“Changes affecting certification”), the Board observes that there is no reference to the change procedures to be agreed, as per section 7.10 of the Annex. The Board encourages the IE SA to include such reference and mention some of the procedures that could be put in place (e.g. transition periods, approvals process with the competent SA...). Additionally, the Board considers that changes in the state of art are also relevant and might affect certification. Therefore, the Board encourages the IE SA to include this possibility among the list of changes affecting certification. Finally, the Board welcomes the inclusion of personal data breaches and infringements of the GDPR in the list of changes that can affect

certification. However, in order to ensure clarity, the Board encourages the IE SA to specify that the data breaches or infringements of the GDPR shall be taken into account only inasmuch as they relate to the certification.

19. Regarding the changes affecting certification (subsection 7.10 of the IE SA's draft requirements) and, in particular, the fifth bullet point, the Board notes that the IE SA refers to "applicable binding decisions of the European Data Protection Board" and also to Article 39 of the EDPB Rules of Procedure, which includes "all final documents adopted by the EDPB". In order to ensure a clear understanding of what is meant by "decisions of the European Data Protection Board", the Board encourages the IE SA to clarify the reference. An example could be to refer to "documents adopted by the European Data Protection Board".
20. The Board observes that subsection 7.11 of the IE SA's draft requirements (termination, restriction, suspension or withdrawal of certification) does not contain the obligation of the certification body to accept decisions and orders from the IE SA to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met. Therefore, the Board recommends the IE SA to include such obligation.

3 CONCLUSIONS / RECOMMENDATIONS

21. The draft accreditation requirements of the Irish Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
22. Regarding 'process requirements' the board recommends that the IE SA:
 - 1) include, in subsection 7.11, the obligation of the certification body to accept decisions and orders from the IE SA to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met.

4 FINAL REMARKS

23. This opinion is addressed to the IE SA and will be made public pursuant to Article 64 (5)(b) GDPR.
24. According to Article 64 (7) and (8) GDPR, the IE SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
25. The IE SA shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 15/2020 on the draft decision of the competent supervisory authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 25 May 2020

Table of contents

1	SUMMARY OF THE FACTS	4
2	ASSESSMENT	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX	6
2.2.2	TERMS AND DEFINITIONS	6
2.2.3	GENERAL REMARKS	6
2.2.4	GENERAL REQUIREMENTS FOR ACCREDITATION (Chapter 4 of the draft accreditation requirements)	7
2.2.5	RESOURCES REQUIREMENTS (Chapter 6 of the draft accreditation requirements)	8
2.2.6	PROCESS REQUIREMENTS (Chapter 7 of the draft accreditation requirements).....	9
2.2.7	FURTHER ADDITIONAL REQUIREMENTS.....	11
3	CONCLUSIONS / RECOMMENDATIONS.....	11
4	FINAL REMARKS	12

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex 1 to the EDPB Guidelines 4/2018 on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The German Supervisory Authorities of the Federation and the Länder (hereinafter “DE SAs”) have submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 13 February 2020. The DE national accreditation body (NAB), DAkkS, will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the DE SAs, once they are approved by the DE SAs, following an opinion from the Board on the draft requirements, to accredit certification bodies.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the DE SAs have decided to resort to joint accreditation by their national accreditation body (NAB), the DAkkS, and the competent

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

SA, for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used when issuing accreditation.

4. This assessment of DE SAs' additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SAs in a way that enables their practical and consistent application as required by the SAs' context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs and the competent SAs, when applicable, when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the DE SAs' draft accreditation requirements, it should be read as the Board not having any comments and not asking the DE SAs to take further action.
9. This opinion does not reflect upon items submitted by the DE SAs, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- 1) addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- 2) independence of the certification body
- 3) conflicts of interests of the certification body
- 4) expertise of the certification body
- 5) appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- 6) procedures for issuing, periodic review and withdrawal of GDPR certification; and

- 7) transparent handling of complaints about infringements of the certification.
10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
 - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
 - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
 - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
 - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

2.2.1 PREFIX

11. The Board acknowledges the fact that terms of cooperation, regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

2.2.2 TERMS AND DEFINITIONS

12. The Board notes that Chapter 3 (“Definitions”) of the DE SAs’ draft accreditation requirements defines what types of certification schemes are allowed, specifying that they must meet the requirements of DIN EN ISO/IEC 17065. In this regard, it should be pointed out that Sections 5.1 and 5.2 of the EDPB Guidelines spell out already what can be certified under the GDPR in a comprehensive manner. Therefore, the Board acknowledges that the intent of the DE SAs is not to limit what stated in the Guidelines and that the assertions contained in Chapter 3 of the DE SAs’ draft accreditation requirements are to be considered applicable in the context of these accreditation requirements.

2.2.3 GENERAL REMARKS

13. The Board notes that the “general notes” section of the DE SAs’ draft accreditation requirements refer to the “authorization” of the certification criteria by the EDPB “in accordance with Art. 63, 64(1)(c)

GDPR". The Board notes that the GDPR does not give the EDPB the competence to "authorise" certification criteria. However, according to the above-mentioned articles, the EDPB can approve certification criteria. Therefore, the Board recommends the DE SAs to delete the reference to "authorisation by the EDPB", in order to put the draft in line with the wording of the GDPR.

2.2.4 GENERAL REQUIREMENTS FOR ACCREDITATION (Chapter 4 of the draft accreditation requirements)

14. Concerning the requirement of legal responsibility (section 4.1 of the DE SAs' draft accreditation requirements), the Board notes that, in the supporting document, the DE SAs explain that there is an expectation for the certification body to have up to date procedures and, therefore, there's no need to add further requirements on that regard. However, the Board considers that an expectation does not bind certification bodies to have such procedures. As established in section 4.1.1 of the Annex to the Guidelines, certification bodies shall have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation. Moreover, the certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling of client organisation's personal data as part of the certification process. Therefore, the Board recommends the DE SAs to amend the draft requirements in order to align them with the Guidelines.
15. Regarding subsection 4.1.2.2 of the DE SAs' draft accreditation requirements ("certification agreement"), the Board notes that the DE SAs' draft accreditation requirements do not include the obligation to allow full transparency to the competent SA with respect to the certification procedure, including contractually confidential matters. In addition, there is no reference to the obligation of the applicant to provide the certification body with access to its processing activities. Therefore, the Board recommends the DE SAs to include the abovementioned obligations in their draft.
16. The Board observes that the explicit reference to the tasks and powers of the competent SA (3rd indent in section 4.1.2 of the Annex) is not included in subsection 4.1.2.2 of the DE SAs' draft accreditation requirements. The Board is of the opinion that this reference should be added in the draft requirements and, therefore, it recommends the DE SAs to amend the draft accordingly.
17. Moreover, the DE SAs' draft requirements regarding the certification agreement do not include the obligation to allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8) and 43(5) GDPR (7th indent in section 4.1.2 of the Annex). Even though that obligation is included in the process management section of the DE SAs' draft accreditation requirements, the Board considers that it should be part of the certification agreement, in order to strengthen its binding nature. Thereby, the Board recommends the DE SAs to include the abovementioned obligation as part of the elements of the certification agreement.
18. According to the Annex, the applicant has to inform the certification body of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification (10th indent in section 4.1.2 of the Annex). However, in the DE SAs' draft accreditation requirements, indent 6 of subsection 4.1.2.2 only includes the obligation to inform the certification body of significant changes in actual or legal circumstances, but it does not explicitly mention the products, processes and services. The Board recommends the DE SAs to include such reference, in line with the Annex.
19. With regard to subsection 4.2.7 of the DE SAs' draft accreditation requirements ("handling impartiality"), the Board recommends to strengthen the criteria applicable to certification bodies

which belong to or are controlled by a separated legal entity, so as to take into consideration that any type of economic relation between the certification body and the legal entity, depending on its features, may affect the impartiality of its certification activities.

20. With regard to section 4.6 of the DE SAs' draft accreditation requirements ("publicly accessible information"), the Board notes that there is no reference to the publication of all versions of the approved criteria and the certification procedures. Therefore, the Board encourages the DE SAs to amend the draft accreditation requirements in order to make explicit that the publication includes all versions of the approved criteria and the certification procedures. Additionally, the Board notes that the second paragraph of section 4.6 states that "the certification schemes used by the certification body the approved criteria in accordance with Art. 42(5) GDPR stating the authorized duration of application, *are to be generally published*." To avoid any ambiguity, the Board encourages the DE SAs to delete the word "generally" and to include an "and" between "certification body" and "the approved criteria".

2.2.5 RESOURCES REQUIREMENTS (Chapter 6 of the draft accreditation requirements)

21. Concerning the expertise requirements and specifically, subsection 6.1.2.1 of the DE SAs' draft accreditation requirements ("human resources competence"), the Board notes that the required knowledge in the listed areas does not specify that the knowledge shall be relevant and appropriate. In order to ensure consistency with the level of expertise required in the Annex, the Board recommends the DE SAs to align the wording with the Guidelines, by requiring that the knowledge is relevant and appropriate.
22. Moreover, the Board notes that the requirements for personnel with technical expertise responsible for decision making include at least 7 years of professional experience or 5 years of professional experience in technical data protection, depending on their level of education, whereas the personnel responsible for evaluations should have 4 years of professional experience or 2 years of professional experience in technical data protection and experience in the testing procedure, depending on their level of education. Similarly, personnel with legal expertise making decisions must have at least 5 years of professional experience in data protection law, whereas those in charge of evaluations must have at least 2 years of experience in data protection law and in the audit procedures. The Board notes that the required minimum years of professional experience between the personnel in charge of decision-making and the personnel in charge of evaluation differ significantly. In this regard, the Board considers that the competence requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform, rather than the number of years of experience. The Board is of the opinion that evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the DE SAs to make more emphasis on the different substantive knowledge and/or experience for evaluators and decision-makers and to reduce the divergences in the years of experience required for them.
23. Additionally, the Board considers that the knowledge of the management systems relevant to the certification area should be extended to the ISO/IEC 27701:2019 - Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines and encourages the DE SAs to include such reference.

24. Finally, regarding the education requirements for the technical personnel, the Board considers that the list of subjects is already tailored to the technical expertise required by the Annex. Therefore, the Board encourages the DE SAs to delete the reference to “natural sciences” from the list of subjects regarding the university education of the technical personnel.

2.2.6 PROCESS REQUIREMENTS (Chapter 7 of the draft accreditation requirements)

25. The Board notes that Chapter 7 of the DE SAs’ draft accreditation requirements makes several reference to the term “its criteria” (e.g. in sections 7.4, 7.6, 7.11 and 7.13). In order to avoid any ambiguity, the Board encourages the DE SAs to clarify the meaning of such term, for example by adding an explanation in Appendix 1 (Glossary).
26. Concerning section 7.1 of the DE SAs’ draft accreditation requirements (“general information”), the Board notes that there is no explicit reference to the obligation of the certification body to comply with the additional requirements. Even though such obligation could be inferred from the text of the draft requirements, the Board considers that an explicit reference to the above-mentioned obligation should be included. Therefore, the Board recommends the DE SAs to amend the draft accordingly.
27. The Board notes that the DE SAs’ draft additional requirements do not contain any reference to the operation of an approved European Data Protection Seal, as per section 7.1.2 of the Annex. The Board is of the opinion that this reference should be included, especially considering that accreditation of a certification body granting European Data Protection Seals may have to be carried out in each of the Members States where the certification body is established.³ Therefore, the Board recommends the DE SAs to include the above-mentioned reference. For example, the draft requirements could state the following: *“The competent SA shall be notified before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office”*.
28. The Board notes that in section 7.2 (“application”), the DE SAs’ draft accreditation requirements foresee the situation in which processors are used to carry out data processing operations, in line with the Annex to the Guidelines. However, the Board notes that, when processors are used, the application shall contain the relevant controller/processor contract(s), as stated in the Annex. Therefore, the Board recommends the DE SAs to align the wording to the guidelines by including the reference to the controller/processor contract(s). Moreover, the Board encourages the DE SAs to consider whether a reference to joint controllers and their specific arrangements should also be mentioned in this case.
29. The Board notes that section 7.2 of the DE SAs’ draft accreditation requirements specifies that “the data controller and the processor are entitled to apply for certification”. The possibility for processors to apply for certification will depend on the specific certification scheme. Therefore, in order to avoid confusion, the Board encourages the DE SAs to delete the reference above or to clarify that the possibility for processors to be certified will depend on the scope of the certification scheme.
30. With regard to section 7.3 of the DE SAs’ draft accreditation requirements (“evaluation applications”), the Board notes that the DE SAs’ draft accreditation requirements state that “the planned evaluation methods are contractually stipulated [...]. In order to make clear that this is a requirement, the Board encourages the DE SAs to redraft the first paragraph, in order to make clear that the evaluation methods shall be included in the certification agreement, -i.e. redraft the requirement as “the planed

³ In this regard, see Guidelines 1/2018, paragraph 44.

evaluation methods shall be contractually stipulated [...]"'. Additionally, the Board encourages the DE SAs to replace the reference to section 7.3.1.b of ISO 17065 with section 7.3 of ISO 17065, in order to align the wording with the Annex. Moreover, the Board observes that the 4th paragraph refers to appropriate technical and legal competences. For the sake of clarity, the Board encourages the DE SAs to add "in the field of data protection".

31. The Board observes that section 7.4 of the DE SAs' draft accreditation requirements ("evaluation methods") does not include the obligation of the certification body to describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria. The Board recommends the DE SAs to amend the draft requirements in order to include such reference. An example could be to add the following: "*The certification body shall ensure that mechanisms used for granting certification describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria*". Moreover, with regard to the first area that shall be covered in the evaluation methods, the Board considers that the necessity and proportionality shall be assessed also in relation to the data subjects concerned, where applicable. Finally, the Board notes that there is no reference to the documentation of methods and findings. Thus, the Board encourages the DE SAs to amend the draft and explicitly include such references.
32. With regard to existing certifications (section 7.4 of the DE SAs' draft accreditation requirements), the Board considers that the 4th indent in page 13 leads to confusion, since it is unclear what is the connection between the periods of validity of current and previous certification, and how they would fit in with one another. Additionally, it does not seem feasible to question the validity of certification previously issued by a different accredited certification body. In sum, the paragraph would benefit from some clarity with regard to the relationship between the different elements mentioned. The Board recommends the DE SAs to amend the draft in particular by clarifying that the duration of validity of the GDPR certification must not be conditional upon the validity of other types of certifications.
33. Concerning section 7.5 ("valuation") of the DE SAs' draft accreditation requirements, the Board encourages the DE SAs to change the title of the section to "review".
34. Regarding the changes affecting certification (section 7.10 of the DE SAs draft accreditation requirements), the Board notes that the DE SAs draft accreditation requirements establish that "the client is informed in a timely manner on changes to the legal framework which affect him". Having in mind the need to preserve the impartiality of the certification body, the Board encourages the DE SAs to reformulate the sentence to make clear that the client is provided, in a timely manner, with general information on changes that might affect him. Additionally, in order to ensure a clear understanding of what is meant by "decisions of the European Data Protection Board", the Board encourages the DE SAs to clarify the reference. An example could be to refer to "documents adopted by the European Data Protection Board".
35. The Board observes that section 7.11 of the DE SAs' draft accreditation requirements ("termination, restriction, suspension or withdrawal of certification") does not contain the obligation of the certification body to accept decisions and orders from the DE SAs to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met. Therefore, the Board recommends the DE SAs to include such obligation. Moreover, the Board encourages the DE SAs to replace the word "restriction" by "reduction" from the title of the section, in accordance with the Annex to the Guidelines.

2.2.7 FURTHER ADDITIONAL REQUIREMENTS

36. With regard to subsection 8.11.3 of the DE SAs' accreditation requirements ("complaint management"), the Board encourages the DE SAs to replace the reference to "justified complaints" by "substantiated complaints", in order to provide more clarity.

3 CONCLUSIONS / RECOMMENDATIONS

37. The draft accreditation requirements of the German Supervisory Authorities of the Federation and the Länder may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:

38. Regarding 'general remarks', the Board recommends that the DE SAs:

- 1) delete the reference to "authorisation by the EDPB", in order to put the draft in line with the wording of the GDPR.

39. Regarding 'general requirements for accreditation', the Board recommends that the DE SAs:

- 1) amend the requirements concerning the legal responsibility (subsection 4.1) in order to align them with the guidelines.
- 2) amend subsection 4.1.2.2 to include, in the certification agreement, the obligation to allow full transparency to the DE SAs with respect to the certification procedure and to provide the certification body with access to the applicant's processing activities.
- 3) include, in subsection 4.1.2.2, an explicit reference to the tasks and powers of the competent SA, in accordance with the Annex.
- 4) include, among the elements of the certification agreement, the obligation to allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8) and 43(5) GDPR.
- 5) include a explicit reference to "products, processes and services concerned by the certification" in indent 6 of subsection 4.1.2.2.
- 6) to strengthen, in subsection 4.2.7, the criteria applicable to certification bodies which belong to or are controlled by a separated legal entity, so as to take into consideration that any type of economic relation between the certification body and the legal entity, depending on its features, may affect the impartiality of its certification activities.

40. Regarding 'resource requirements' the board recommends that the DE SAs:

- 1) align the wording of subsection 6.1.2.1 with the guidelines, by requiring that the knowledge is relevant and appropriate.

41. Regarding 'process requirements' the board recommends that the DE SAs:

- 1) amend section 7.1 to contain an explicit reference to the obligation of the certification body to comply with the additional requirements.

- 2) include a reference to the operation of an approved European Data Protection Seal.
- 3) align the wording in section 7.2 to the guidelines by including the reference to the controller/ processor contract(s).
- 4) include in section 7.4 the obligation of the certification body to describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria.
- 5) clarify in section 7.4 that the duration of validity of the GDPR certification must not be conditional upon the validity of other types of certifications.
- 6) include in section 7.11 the obligation of the certification body to accept decisions and orders from the DE SAs to withdraw or not to issue certification to an applicant if the requirements for certification are no longer met.

4 FINAL REMARKS

42. This opinion is addressed to the German Supervisory Authorities of the Federation and the Länder and will be made public pursuant to Article 64 (5)(b) GDPR.
43. According to Article 64 (7) and (8) GDPR, the DE SAs shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether they will amend or maintain their draft decision. Within the same period, they shall provide the amended draft decision or where they do not intend to follow the opinion of the Board, they shall provide the relevant grounds for which they do not intend to follow this opinion, in whole or in part.
44. The DE SAs shall communicate the final decision to the Board for inclusion in the register of decisions that have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 16/2020 on the draft decision of the competent supervisory authority of the Czech Republic regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 25 May 2020

Table of contents

1	SUMMARY OF THE FACTS	4
2	ASSESSMENT	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX	6
2.2.2	GENERAL REMARKS	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION	7
2.2.4	RESOURCE REQUIREMENTS.....	8
2.2.5	PROCESS REQUIREMENTS.....	8
2.2.6	MANAGEMENT SYSTEM.....	10
3	CONCLUSIONS / RECOMMENDATIONS.....	10
4	FINAL REMARKS	11

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Czech Supervisory Authority (hereinafter “CZ SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 17 February 2020. The CZ national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the CZ SA, once they are approved by the CZ SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the CZ SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

4. This assessment of CZ SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
7. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the CZ SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the CZ SA to take further action.
9. This opinion does not reflect upon items submitted by the CZ SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
 - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
 - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
 - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
 - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

2.2.1 PREFIX

11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

2.2.2 GENERAL REMARKS

12. The Board notes that the draft accreditation requirements do not completely follow the structure set out in Annex 1 to the Guidelines. For example, the sections on “scope” and “terms and definitions” are missing. In this regard, for the sake of clarity and to allow for an easier assessment of the requirements, the Board considers that the numbering and the overall structure of the document could be improved. Therefore, with the aim to facilitate the assessment, the Board encourages the CZ SA to follow the structure of the Annex in the draft accreditation requirements and add the missing sections, being of special relevance the definition of the terms used throughout the document. Moreover, the Board notes that the CZ SA’s draft accreditation requirements refer several times to the respective ISO 17065 section or to the respective sections of the Annex, without specifying however such reference. Thus, the Board encourages the CZ SA to make clear the references to the sections of the ISO 17065 and of the Annex.

13. The Board notes that the CZ SA's draft accreditation requirements refer several times to the "evaluated object" (e.g. sections 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 and 3.2.1.2.10.10.2). The Board understands that this term is used as a synonym for the "target of evaluation". However, in order to ensure clarity, the Board encourages the CZ SA to use the term "target of evaluation" consistently.
14. The Board notes that several requirements are not formulated as an obligation of the certification body (e.g. 3.2.1.2.2 and 3.2.1.2.3). The Board encourages the CZ SA to redraft the requirements to make clear that they are mandatory -i.e. start the requirement with 'the certification body shall [...]'.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

15. Concerning the certification agreement (section 3.2.1.2.1.2 of the CZ SA's draft accreditation requirements), the Board notes that subsection 3.2.1.2.1.2.2 does not make any reference to the "contractually confidential matters", to which the SA shall also have access. Therefore, the Board recommends the CZ SA to amend the draft, by including the obligation to provide access to the SA to contractually confidential matters as well.
16. With regard to subsection 3.2.1.2.1.2.8 of the CZ SA's draft accreditation requirements, the Board notes that it is unclear as to whom the information shall be disclosed. Therefore, the Board encourages the CZ SA to clarify who will be the recipient of the information. Moreover, the information referred shall be "necessary for granting certification", as set out in section 4.1.2 point 7 of the Annex. The Board recommends the CZ SA to replace "information about granting certification" by "information necessary for granting certification".
17. Regarding subsection 3.2.1.2.1.2.9 of the CZ SA's draft accreditation requirements, it is unclear what type of information should be communicated directly to the Board. Article 42(8) GDPR sets out an obligation for the Board to collate, *inter alia*, all certification mechanisms. In this context, it is assumed that the competent SAs will provide the relevant information to the Board, who will then publish it on the public register. Therefore, the Board recommends the CZ SA to clarify subsection 3.2.1.2.1.2.9 of the draft requirements in line with Article 42(8) GDPR.
18. Concerning subsection 3.2.1.2.1.2.12 of the CZ SA's draft accreditation requirements, the Board takes note of the fact that the CZ SA created a reworded version of part of the requirement foreseen in the Annex. The CZ SA, however, omitted a reference to [where applicable] "the consequences for the customer should also be addressed". The Board therefore recommends the CZ SA to add the missing part of the requirement mentioned above.
19. Additionally, subsection 3.2.1.2.1.2.13 of the CZ SA's draft accreditation requirements establishes the obligation to "contain a commitment of the applicant to inform the certification body about all changes that may affect compliance of the certificated object with the certification criteria". The Board considers this formulation too generic, and recommends the CZ SA to amend the draft requirements in order to include "all changes in its actual or legal situation and in its products, processed and services concerned by the certification".
20. Concerning the use of data protection seals and marks (section 3.2.1.2.1.3 of the CZ SA's draft accreditation requirements), the Board notes that the CZ SA's draft requirements establish that the certification agreement shall contain "rules of using certificates, seals and marks if provided by the certification scheme owner". The same formulation is found in subsection 3.2.1.2.1.2.14. The Board considers that this obligation is already covered by item 4.1.2.2. letter I) of ISO 17065 and, therefore,

it should be contained in any certification scheme (see also item 4.1.3 of ISO 17065). Thus, for the sake of clarity, the Board recommends the CZ SA to delete the aforementioned sections.

21. With regard to the requirements on the management of impartiality, according to the information provided by the CZ SA in the template, section 4.2.1.b) and 4.2.2 of the Annex are sufficiently covered by item 4.2 of ISO 17065. However, the Board considers that these requirements shall be explicitly included in the draft accreditation requirements developed by the SAs in line with the Annex. Therefore, the Board recommends the CZ SA to include the missing requirements regarding the management of impartiality foreseen in the Annex.
22. With regard to the requirement on liability and financing (section 3.2.1.2.3.1 of the CZ SA's draft requirements), the Board encourages the CZ SA to specify that it has to be ensured on a regular basis.

2.2.4 RESOURCE REQUIREMENTS

23. Concerning certification body personnel (section 3.2.1.2.8.1.6 of the CZ SA's draft accreditation requirements), the Board notes that the requirements for personnel responsible for evaluations (subsection 3.2.1.2.8.1.6.3) include "5-year practice with at least 10 performed audits carried out within certification activity in the same or similar field [...] or 5-year practice within certification of the objects of certification body focus". Similarly, the requirements for personnel responsible for decision-making (subsection 3.2.1.2.8.1.6.4) include "at least 5-year practice with at least 10 performed audits carried out within certification activity in the same or similar field". The Board considers that the expertise requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In this regard, the Board is of the opinion that evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the CZ SA to redraft this subsection taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.
24. Furthermore, the Board takes note that point 3.2.1.2.9.1 of the CZ SA's draft accreditation requirements states that outsourcing is not allowed for certification activities. However, the following point allows the use of external auditors and external experts for evaluation, unless it constitutes certification activities. The Board considers that the draft accreditation requirements should specify when "it constitutes certification activities" or clarify that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the CZ SA to amend the draft accordingly.

2.2.5 PROCESS REQUIREMENTS

25. The Board notes that section 3.2.1.2.10.1.1 of the CZ SA's draft additional requirements refer to "all the additional requirements concerning a conflict of interests (7.1 point 1)". However, the CZ SA's draft additional requirements do not contain additional requirements concerning conflict of interest. Therefore, the Board encourages the CZ SA to amend the draft in order to avoid confusion.
26. With regard to the application requirements, the Board notes that subsection 3.2.1.2.10.2.3 of the CZ SA's draft accreditation requirements seems to imply that information on the transferred data shall only be provided in the application when the transfer is to a third country or international

organisation. However, the Board underlines that the applicant shall always contain a description of the data transferred to other systems or organisations, regardless of their location. Therefore, the Board encourages the CZ SA to amend the wording in order to avoid confusion.

27. The Board notes that the obligation to lay down in the certification agreement the binding evaluation methods (section 3.2.1.2.1.2.6 of the CZ SA's draft accreditation requirements) does not contain a reference to the Target of Evaluation, as per item 1 section 7.3 of the Annex to the Guidelines. For clarity purposes, the Board encourages the CZ SA to include such reference.
28. Moreover, the Board notes that CZ SA's draft accreditation requirements foresee the situation in which processors are used to carry out data processing operations, in line with the Annex to the Guidelines (section 3.2.1.2.10.2 of the CZ SA's draft accreditation requirements). The Board encourages the CZ SA to consider whether a reference to joint controllers and their specific arrangements should also be mentioned in this case.
29. Regarding the evaluation requirements (section 3.2.1.2.10.4 of the CZ SA's draft requirements), the Board notes that the CZ SA's accreditation requirements do not contain the obligation of the certification body to set out in detail in its certification mechanism how the information required in item 7.4.6 ISO 17065 shall be provided to the applicant about non conformities from a certification mechanism. As set out in the Annex (subsection 7.4), at least the nature and timing of such information shall be defined. Therefore, the Board recommends the CZ SA to add the aforementioned obligation.
30. Moreover, subsection 3.2.1.2.10.4.2 of the CZ SA's draft requirements seems to limit the evaluation methods to testing, auditing or inspections. The Board considers that other evaluation methods could also be used and, therefore, it encourages the CZ SA to amend the draft in order to make clear that the enumeration is not exhaustive.
31. Concerning subsection 3.2.1.2.10.4.4.1.4 of the CZ SA's draft accreditation requirements, the Board considers that the requirements should clearly state that the certification body is obliged to check the compliance with the criteria, and encourages the CZ SA to amend the draft accordingly.
32. With regard to the review requirements (subsection 3.2.1.2.10.5 of the CZ SA's draft accreditation requirements), the Board observes that the CZ SA's draft accreditation requirements do not make reference to the obligation to set out procedures for the granting and revocation of certifications. The Board recommends the CZ SA to amend the draft accordingly.
33. Concerning the requirements on certification documentation, the Board notes that section 3.1.2.10.7.2 of the CZ SA's draft accreditation requirements states that the certification body shall specify that monitoring is a condition of validity of certification "if monitoring required by a certification scheme [...]". The Board considers that, in the case of certification under the GDPR, the monitoring activities are always mandatory and, therefore, recommends the CZ SA to include such obligation.
34. With regard to the requirements related to the directory of certified products (section 3.2.1.2.10.8 of the CZ SA's draft accreditation requirements and 7.8 of the Annex), and particularly, the obligation to inform the competent SA of the reasons for granting or revoking the requested certification, the Board notes that the CZ SA's draft accreditation requirements refer to section 3.2.1.2.10.4.5. However, such section concerns the obligation to make the evaluation documentation accessible to the CZ SA upon request, whereas the requirement in section 7.8 of the Annex to the Guidelines contains an obligation

to proactively inform the SA of the reasons for granting or revoking the certification. Therefore, the Board recommends the CZ SA to amend the draft accordingly.

35. Regarding the changes affecting certification, the Board notes that the CZ SA's draft accreditation requirements do not mention, among the procedures to be agreed, the approval process with the competent SA, referenced in the Annex to the Guidelines (page 19). The Board acknowledges that the list provided in section 7.10 of the Annex is not mandatory. However, in order to ensure consistency, the Board encourages the CZ SA to add a reference to the approval process with the SA.
36. The Board observes that the CZ SA's draft accreditation requirements do not clearly include the obligation of the certification body to accept decisions and orders from the competent SA to withdraw or not to issue certification to an applicant if the requirements for certification are no longer met. The Board recommends the CZ SA to clearly include such obligation in the draft accreditation requirements. With regard to the termination, reduction, suspension or withdrawal of certification, the Board notes that sections 3.2.1.2.10.10.2 and 3.2.1.2.10.10.3 of the draft requirements refer to an "instigation". If the intention is to refer to "decisions and orders" from the SA, as established in article 58(2)(h) GDPR, the Board encourages the CZ SA to use the same terminology as the GDPR, and refer to "decisions and orders".

2.2.6 MANAGEMENT SYSTEM

37. The Board considers that section 3.2.1.2.11 of the CZ SA's draft additional requirements do not contain the obligation of the certification body to "make public permanently and continuously which certifications were carried out on which basis, how long the certifications are valid under which framework and conditions", as stated in section 8 of the Annex. Therefore, the Board recommends the CZ SA to amend the draft requirements by including the abovementioned reference.

3 CONCLUSIONS / RECOMMENDATIONS

38. The draft accreditation requirements of the Czech Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
39. Regarding 'general requirements for accreditation', the Board recommends that the CZ SA:
 - 1) include the obligation to provide access to the SA to "contractually confidential matters" in section 3.2.1.2.1.2.
 - 2) replace "information about granting certification" with "information necessary for granting certification" in subsection 3.2.1.2.1.2.8.
 - 3) clarify subsection 3.2.1.2.1.2.9 in line with Article 42(8) GDPR.
 - 4) in subsection 3.2.1.2.1.2.12, add a reference to [where applicable] "the consequences for the customer should also be addressed".
 - 5) amend subsection 3.2.1.2.1.2.13 to include "all changes in its actual or legal situation and in its products, processed and services concerned by the certification".
 - 6) delete section 3.2.1.2.1.3 and subsection 3.2.1.2.1.2.14.

- 7) include the missing requirements regarding the management of impartiality foreseen in the Annex.
40. Regarding ‘resource requirements’, the Board recommends that the CZ SA:
- 1) amend section 3.2.1.2.9.1 to specify when “it constitutes certification activities” or clarify that the certification body will retain the responsibility for the decision-making, even when it uses external experts.
41. Regarding ‘process requirements’, the Board recommends that the CZ SA:
- 1) include, in section 3.2.1.2.10.4, the obligation of the certification body to set out in detail in its certification mechanism how the information required in item 7.4.6 ISO 17065 shall be provided to the applicant about non conformities from a certification mechanism.
 - 2) amend section 3.2.1.2.10.5 to make reference to the obligation to set out procedures for the granting and revocation of certifications.
 - 3) amend section 3.1.2.10.7.2 to reflect that in the case of certification under the GDPR, the monitoring activities are always mandatory.
 - 4) amend section 3.2.1.2.10.8 to reflect the obligation of the certification body to proactively inform the SA of the reasons for granting or revoking the certification.
 - 5) include the obligation of the certification body to accept decisions and orders from the competent SA to withdraw or not to issue certification to an applicant if the requirements for certification are no longer met.
42. Regarding ‘management system’, the Board recommends that the CZ SA:
- 1) include the obligation of the certification body to “make public permanently and continuously which certifications were carried out on which basis, how long the certifications are valid under which framework and conditions”, as stated in section 8 of the Annex.

4 FINAL REMARKS

43. This opinion is addressed to the Czech Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
44. According to Article 64 (7) and (8) GDPR, the CZ SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
45. The CZ SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair
(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 17/2020 on the draft Standard Contractual Clauses
submitted by the SI SA (Article 28(8) GDPR)**

Adopted on 19 May 2020

TABLE OF CONTENTS

1	Summary of the Facts	4
2	Assessment	4
2.1	General reasoning of the Board regarding the set of standard contractual clauses	4
2.2	Analysis of the draft standard contractual clauses	5
2.2.1	General remark on the whole SCCs	5
2.2.2	Preamble (Clause 1 of the SCCs).....	5
2.2.3	The data processor acts according to instructions (Clause 3 of the SCCs).....	6
2.2.4	Confidentiality (Clause 4 of the SCCs).....	6
2.2.5	Security of processing (Clause 5 of the SCCs and Appendix C.2)	6
2.2.6	Transfer of data to third countries or international organisations (Clause 7 and Appendix C.6 of the SCCs)	7
2.2.7	Assistance to the data controller (Clause 8 and Appendix C.3 of the SCCs)	7
2.2.8	Notification of personal data breach (Clause 9 of the SCCs).....	7
2.2.9	Erasure and return of data (Clause 10 of the SCCs and Appendix C.4)	7
2.2.10	Audit and inspection (Clause 11 of the SCCs and Appendixes C.7 and C.8)	8
2.2.11	Commencement and termination (Clause 13 of the SCCs)	8
2.2.12	Data controller and data processor contacts / contact points (Clause 14 of the SCCs)..	8
2.2.13	Appendix A	8
2.2.14	Appendix B	9
3	Conclusions	9
4	Final Remarks	9

The European Data Protection Board

Having regard to Article 28(8), Article 63 and Article 64(1)(d), (3) - (8) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter, "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter, the "Board") is to ensure the consistent application of the GDPR throughout the Union. To this end, the Board shall issue an opinion based on Article 64(1)(d) GDPR where a supervisory authority (hereinafter, "SA") aims to determine standard contractual clauses (hereinafter, also "SCCs") referred to in Article 28(8) GDPR. The aim of this Opinion is therefore to contribute to a harmonised approach concerning measures to be adopted by a supervisory authority that are intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States and the consistent implementation of the GDPR's specific provisions.
- (2) In the context of the relationship between a data controller and a data processor (or data processors) for the processing of personal data, the GDPR establishes, in its Article 28, a set of provisions with respect to the setting up of a specific contract between the parties involved and to mandatory provisions that should be incorporated in it.
- (3) According to Article 28(3) GDPR, the processing by a data processor "*shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller*"; a set of specific aspects to regulate the contractual relationship between the parties is therefore set out, including among others, the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects.
- (4) Under Article 28(6) GDPR, without prejudice to an individual contract between the data controller and the data processor, the contract or the other legal act referred in paragraphs (3) and (4) of Article 28 GDPR may be based, in whole or in part, on standard contractual clauses. These standard contractual clauses are to be adopted for the matters referred to in paragraphs (3) and (4).
- (5) Furthermore, Article 28(8) GDPR determines that a SA may adopt a set of standard contractual clauses in accordance with the consistency mechanism referred to in Article 63. In this regard, SAs are required to cooperate with other members of the Board and, where relevant, with the European Commission through the consistency mechanism. Pursuant to Article 64(1)(d), SAs are required to communicate to the Board any draft decision aiming to determine standard contractual clauses

¹ References to the "Union" made throughout this Opinion should be understood as references to the "EEA".

pursuant to Article 28(8). In this context, the Board is required to issue an opinion on the matter, pursuant to Article 64(3), where it has not already issued an opinion on the same matter.

(6) Adopted standard contractual clauses constitute a set of guarantees to be used as is, as they are intended to protect data subjects and mitigate specific risks associated with the fundamental principles of data protection.

(7) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Slovenian supervisory authority (hereinafter, “SI SA”) has submitted its draft decision and its draft standard contractual clauses to the Board, requesting its opinion pursuant to Article 64(1)(d), for a consistent approach at Union level. The decision on the completeness of the file was taken on 21 February 2020. The EDPB Secretariat circulated the file to all members on behalf of the Chair on 21 February 2020.
2. The Board has received the draft SCCs from the SI SA along with a draft decision explaining the background and structure of the standard contractual clauses. These two documents were provided by the Slovenian SA in an English version.
3. In compliance with Article 10(2) of the Board Rules of Procedure², due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks (until 29 May 2020).

2 ASSESSMENT

2.1 General reasoning of the Board regarding the set of standard contractual clauses

4. Any set of standard contractual clauses submitted to the Board under Article 28(8) and Article 64(1)(d) must further specify the provisions foreseen in Article 28 GDPR. The opinion of the Board aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented draft clauses, which could serve as Art. 28(8) standard contractual clauses.
5. The Board notes that the draft SCCs presented to the Board are composed of two parts:

² Version 6, as last modified and adopted on 29 January 2020.

- 1) a general part containing general provisions to be used “as is”; and
 - 2) a specific part that has to be completed by the parties with regard to the specific processing which the contract seeks to govern.
6. In addition, the SI SA explains, in its draft decision, that the model contract (SCCs) “addresses the main issues that are frequently discussed by the controllers and processors when determining their mutual rights and obligations”, and that more specifically it “primarily addresses the content, set out in Article 28(3) GDPR” but it “also addresses issues that can, in line with [their] experience, cause uncertainty among the parties and need special attention”.
7. Among the elements to be taken into account by the Board, the SI SA specified to the EDPB members in its request that it followed the example of the SCCs submitted by the Danish SA³ and considered Opinion 14/2019 of the EDPB, adopted on 9 July 2019 by the EDPB⁴. The Board recognises that the SI SA has taken into account the referred Opinion already adopted by the Board on draft SCCs for the purposes of compliance with Article 28 GDPR and recalls that the evaluation of each draft decision subject to the consistency mechanism is made individually and on its own merits, bearing in mind the goal of ensuring consistency.
8. When this opinion remains silent on one or more clauses of the SCCs submitted by the SI SA, it means that the Board is not asking the SI SA to take further action with regard to those specific clauses.

2.2 Analysis of the draft standard contractual clauses

2.2.1 General remark on the whole SCCs

9. Since a contract under Article 28 GDPR should further stipulate and clarify how the obligations in Article 28(3)-(4) will be fulfilled, the SCCs need to be analysed in their entirety.
10. In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority does not prevent the parties from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the adopted standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Furthermore, where the standard data protection clauses are modified, the parties will no longer be deemed to have implemented adopted standard contractual clauses.

2.2.2 Preamble (Clause 1 of the SCCs)

11. Regarding **clause 1.5** of the SCCs, the Board notes that other goals are also pursued through standard contractual clauses adopted for the purpose of Article 28. Thus, the Board encourages the SI SA to rephrase the sentence as follows: *“The Clauses are intended to protect the rights of the data subjects, mitigate specific data protection risks and ensure clarity in the relationship between the controller and the processor and as to the respective rights and duties”*.

³ The final version of the standard contractual clauses for the purposes of compliance with Article 28 GDPR adopted by the Danish SA is available here: https://edpb.europa.eu/our-work-tools/our-documents/decision-sa/dk-sa-standard-contractual-clauses-purposes-compliance-art_en.

⁴ EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), adopted on 9 July 2019, available here:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf.

2.2.3 The data processor acts according to instructions (Clause 3 of the SCCs)

12. Regarding **clause 3.1** of the SCCs, the Board encourages the SI SA to add the word “or” in “Union [or] Member State law”.
13. The SCCs specify in **clause 3.3** that “[t]he data processor and, where applicable, the processor’s representative will in accordance with Article 30(2) GDPR maintain a record of all categories of processing activities carried out on behalf of a controller”. While Article 28(3) GDPR does not specifically impose on controllers and processor a duty to include in the contract the obligation for the processor to keep a record under Article 30(2) GDPR, the Board considers this measure as contributing “to demonstrate compliance” and helpful to “assist the controller in ensuring compliance with the obligations pursuant to Article 32 to 36” (Article 28(3)(h) and (f) GDPR).

2.2.4 Confidentiality (Clause 4 of the SCCs)

14. The Board understands that **clause 4.2** of the SCCs refers to the possibility for the controller to ask the processor to demonstrate that the persons under the processor’s authority who have access to the personal data are bound by an obligation of confidentiality and their access to personal data is only granted on a need-to-know basis. Consequently, the Board encourages the SI SA to slightly rephrase the clause in order to clarify it. For instance, the clause could be redrafted as follows: “*The data processor shall, at the request of the data controller, demonstrate that the concerned persons under the data processor’s authority are subject to the abovementioned obligation of confidentiality and are only given access to personal data on a need-to-know basis*”.

2.2.5 Security of processing (Clause 5 of the SCCs and Appendix C.2)

15. With regard to **clause 5.1** of the SCCs, the Board would like to highlight that it is generally not appropriate for standard contractual clauses to merely restate the content of the provisions of the GDPR as they should rather specify the concrete application of relevant obligations. Although this clause is not considered as problematic, the EDPB encourages the SI SA to slightly rephrase it (e.g. “*Pursuant to Article 32 GDPR, which stipulates that [...], the parties shall implement [...]*”).
16. With regard to **clause 5.3⁵** of the SCCs, the Board understands it as referring to a risk assessment independently performed by the processor in order to comply with Article 32 and Recital 83 GDPR. The Board encourages the SI SA to clarify that such assessment refers to the processing entrusted to the processor by the controller and recalls that the controller is anyway not exempt from its obligations to comply with Articles 25, 32, 35, 36 GDPR. For instance, clause 5.3 could be rephrased as follows: “*According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the controller, and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks*”.

⁵ The draft clause 5.3 specifies: “*According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks*”.

17. **Appendix C.2** invites the parties to list the security measures that have been agreed by the parties and need to be implemented by the data processor. The Board recalls that the degree of detail of this information must be such as to enable the controller to assess the appropriateness of the measures and to comply with its obligation of accountability.

2.2.6 Transfer of data to third countries or international organisations (Clause 7 and Appendix C.6 of the SCCs)

18. The Board encourages the SI SA to clarify that the words “third countries” refer to countries outside of the EEA and not outside of Slovenia. This could be carried out by adding in clause 7.1 “[...] *third countries (i.e. countries outside of the European Economic Area) [...]*”.
19. With regard to **clause 7.3** of the SCCs, the Board encourages the SI SA to specify that the reference to the “authorisation” of the controller is not an alternative to the “documented instructions” but rather describes a possible content of such instructions. Additionally, the Board encourages the SI SA to further clarify the relationship among clauses 7.1, 7.2, and 7.3. Consequently, clause 7.3 could be rephrased as follows: “*Without documented instructions from the data controller, e.g. providing for an authorisation, or a specific requirement under EU or Member State law to which the data processor is subject, the data processor cannot within the framework of the Clauses [...]*”.

2.2.7 Assistance to the data controller (Clause 8 and Appendix C.3 of the SCCs)

20. The Board is of the opinion that any reference to a specific national supervisory authority in a model contract should be avoided, since the identification of the competent supervisory authority will depend on the specific processing at stake and on the specific circumstances. Consequently, the Board recommends that the references to the Slovenian SA be removed from **clause 8.2** and be replaced, in both points a. and d., by a blank space accompanied by a note inviting the parties to specify the competent supervisory authority (e.g. “[please indicate the competent SA]”).

2.2.8 Notification of personal data breach (Clause 9 of the SCCs)

21. Regarding **clause 9.3** of the SCCs, the Board recommends that the reference to clause 9.2.a be replaced by a reference to clause 8.2.a. Additionally, the Board recommends that the reference to Appendix D in **clause 9.4** be replaced by a reference to Appendix C.3, and that the reference to clauses 9.1 and 9.2 in **Appendix C.3** be replaced with references to clauses 8.1 and 8.2.
22. With regard to **Appendix C.3**, the Board encourages the SI SA to avoid referring to “the role and obligations of the data processor” in the notes inviting the parties to introduce further specifications, since such broad wording might lead to uncertainty as to how the blank spaces should be filled by the parties. Consequently, the Board suggests referring to the steps to be taken by the processor and the procedure to be followed in providing assistance to the controller (with regard to data breach notifications and data protection impact assessments).

2.2.9 Erasure and return of data (Clause 10 of the SCCs and Appendix C.4)

23. Regarding **clause 10.1** of the SCCs, the Board encourages the SI SA to clarify that the processor should either delete or return the personal data (and delete copies) except for when further storage of the personal data by the processor is required by EU or Member State law. Since the exception to the legal duty refers to both Option 1 and Option 2, the words “*unless Union or Member State law requires*

storage of the personal data" should not be in bold and should be presented in a way to ensure that the parties of the contract do not understand it as only referring to the second option. The Board suggests further specifying this wording (e.g. "*unless Union or Member State law requires further storage of the personal data by the processor*").

24. In **Appendix C.4**, the Board recommends that the example should refer not only to a "time period" but also, alternatively, to an "event" ("(STATE TIME PERIOD / EVENT)") since there could be situations in which the precise time frame cannot be established but the data should be deleted after the occurrence of a specific event. Additionally, Appendix C.4 should refer to clause 10.1 instead of 11.1.

2.2.10 Audit and inspection (Clause 11 of the SCCs and Appendixes C.7 and C.8)

25. The Board recommends that the reference in **clause 11.2** to Appendixes C.6 and C.7 be replaced by a reference to Appendixes C.7 and C.8.
26. Additionally, the Board recalls that the audits referred to in Article 28(3)(h) GDPR are conducted either by the controller himself or by another auditor mandated by the controller. The Board recommends the SI SA to adapt the first scenario in **Appendices C.7 and C.8** to specify that the third party auditor has been mandated by the controller. Consequently, the text of the examples in Appendixes C.7 and C.8 should be changed as follows: "*The data processor shall (STATE TIME PERIOD) at (THE DATA PROCESSOR'S/THE DATA CONTROLLER'S) expense be subject to an (AUDIT/INSPECTION) from an independent third party mandated by the controller concerning the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The independent third party auditor will submit a (AUDITOR'S REPORT/INSPECTION REPORT). The parties have agreed that the following types of (AUDITOR'S REPORT/INSPECTION REPORT) may be used in compliance with the Clauses: (INSERT 'APPROVED' AUDITOR'S REPORTS/INSPECTION REPORTS) [...]*".

2.2.11 Commencement and termination (Clause 13 of the SCCs)

27. Regarding **clause 13.5** of the SCCs, the Board encourages the SI SA to avoid indicating this as a specific clause as it just includes the signature of the parties and suggests that the parties and their signature should be referred to in the same way (e.g. "Name", "Position", "Date", "Signature", removing references to "Telephone number" and "Email" which will already be included in clause 14.2).

2.2.12 Data controller and data processor contacts / contact points (Clause 14 of the SCCs)

28. The Board encourages the SI SA to rephrase clause 14.1 as follows: "*Each party shall designate a person responsible for the execution of the contract*".

2.2.13 Appendix A

29. While noting that Appendix A aims at providing details about the processing activities undertaken by the data processor on behalf of the data controller, the Board recalls that the processing activities should be described by the parties in the most detailed manner possible. It is therefore important that the examples provided to illustrate the possible content of the sections of the Appendix are able to guide the parties' description.
30. In light of the above, the Board welcomes the initiative of the SI SA to include examples in **Appendix A.4** and would even suggest expanding it more, taking into account that most processing operations

involve several categories of data subjects at the same time, which in turn can be categorised in several ways, e.g. customers, consumers (adults / children), third party vendors.

2.2.14 Appendix B

31. The Board encourages the SI SA to clarify that multiple sub-processors can be listed by the parties in **Appendix B.1** although only one field has been included by way of example.

3 CONCLUSIONS

32. The Board very much welcomes the Slovenian SA's initiative to submit its draft SCCs for an opinion which aims at contributing to a harmonised implementation of the GDPR.
33. The Board is of the opinion that the draft SCCs of the Slovenian Supervisory Authority submitted for an opinion need some further adjustments in order to be considered as standard contractual clauses. If all recommendations listed in this Opinion are implemented, the SI SA will be able to use this draft agreement as Standard Contractual Clauses pursuant to Article 28(8) GDPR without any need for a subsequent adoption from the EU Commission.

4 FINAL REMARKS

34. This opinion is addressed to Informacijski pooblaščenec (the Slovenian Supervisory Authority) and will be made public pursuant to Article 64 (5)(b) GDPR.
35. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means, within two weeks after receiving the opinion, whether it will amend or maintain its draft SCCs. Within the same period, it shall provide the amended draft SCCs or, alternatively, the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



Opinion 18/2020 on the draft decision of the competent supervisory authority of the Netherlands regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 23 July 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the NL SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS	5
2.2.2	INDEPENDENCE	6
2.2.3	EXPERTISE	7
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES	8
2.2.5	TRANSPARENT COMPLAINT HANDLING	8
2.2.6	CONFLICT OF INTEREST	9
2.2.7	REVIEW MECHANISMS	9
2.2.8	LEGAL STATUS	10
3	CONCLUSIONS / RECOMMENDATIONS.....	10
4	FINAL REMARKS.....	11

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Dutch Supervisory Authority (hereinafter "NL SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 May 2020.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the NL SA to take further action.
7. This opinion does not reflect upon items submitted by the NL SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the NL SA’s accreditation requirements for Code of Conduct’s monitoring bodies

8. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board observes that, according to the general notes of the draft accreditation requirements, the NL SA reserves the right to conduct a risk-based review of the monitoring body to ensure that the body still meets the requirements for accreditation, whereas such a review could be initiated by (but is not limited to): amendments to the code of conduct, substantial changes to the monitoring body or the monitoring body failing to deliver its monitoring functions. The Board welcomes the provision concerning the re-assessment, according to a risk-based approach, of the accreditation requirements by the NL SA in order to ensure compliance with the GDPR. However, for the sake of clarity and transparency, the Board recommends the NL SA to explicitly state that in case of substantial changes to the monitoring body relating to the monitoring body's ability to function independently and effectively, such a review will be always conducted.
10. The Board encourages the NL SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.

2.2.2 INDEPENDENCE

11. The Board observes that the NL SA's 'explanatory notes' section concerning the requirements for independence, refer to independence "*from the code owner or the code members*". As stated in the Guidelines, the independence of the body concerned should be demonstrated in relation also to the profession, industry or sector to which the code applies (para. 63). Therefore, the Board recommends that the NL SA redraft this reference in line with the Guidelines and put it in the 'requirements' section – so as to clarify that this is a requirement itself.
12. The Board notes that the first paragraph of section 1.1 in the NL SA's draft accreditation requirements fits better into the relevant 'explanatory notes' section. Therefore, the Board encourages the NL SA to appropriately move this paragraph.
13. The Board welcomes the requirement that the legal structure of the monitoring body, including its ownership, must shield the monitoring body from external influence (subsection 1.1.1 in the NL SA's draft accreditation requirements), as well as the provision of relevant examples of how this might be demonstrated. However, the Board encourages the NL SA to clarify that this external influence should be considered with respect to the code owner and the code members. Moreover, with regard to the relevant examples, the Board encourages the NL SA to clarify the term 'articles of incorporation', as well as to add, as a relevant example, that the duration, or expiration of the mandate of the monitoring body should be fixed in such a way as to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely affects the independence in carrying out the monitoring activities by the monitoring body.
14. Furthermore, the Board is of the opinion that internal monitoring bodies can be set up only within a code owner. Therefore, the Board recommends that this is clarified and reflected in the text of the draft accreditation requirements in the subsection 1.1.2 – e.g. by replacing "for example" with "in particular".
15. In subsection 1.1.3 in the NL SA's draft accreditation requirements, it is stated that "*the monitoring body shall demonstrate organisational independence, for example, an internal monitoring body may use different logos or names where appropriate*". The Board welcomes such an example; however, especially for the case of internal monitoring bodies, the Board encourages the NL SA to add more concrete examples of evidence illustrating organizational independence of an internal monitoring body, such as, e.g., information barriers and separate reporting structures.
16. With regard to the legal status and decision-making process (section 1.1 in the NL SA's draft accreditation requirements), the Board acknowledges the impartiality of the monitoring body from the code members. However, the Board is of the opinion that these requirements should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members, as well as with regard to the profession, industry or sector to which the code applies. For this reason, the Board encourages the NL SA to amend this section accordingly.
17. Furthermore, the Board considers that the section concerning the financial independence (section 1.2 in the NL SA's draft accreditation requirements) should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. These include the number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the

processing operation(s). Therefore, the Board encourages the NL SA to redraft the requirements accordingly.

18. Moreover, as for the financial requirements (section 1.2), the Board considers that such requirements would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support should not adversely affect its independence (subsection 1.2.2). For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the NL SA to provide examples of how the monitoring body can provide such evidence.
19. The Board welcomes the provision in the subsection 1.3.1 in the NL SA's draft accreditation requirements that "*the monitoring body shall demonstrate that it has adequate resources and personnel to effectively perform its tasks*". The Guidelines though provide further specialisation on this, stating that the resources should be proportionate to the expected number and seize of code members, as well as the complexity or degree of risk of the relevant data processing. Therefore, the Board encourages the NL SA to redraft this requirement in line with the Guidelines.
20. Moreover, with respect to subsection 1.3.1, the Board encourages the NL SA to include a reference to technical resources necessary for the effective performance of the monitoring body's tasks.
21. Subsection 1.3.3 (under the section on "organisational independence") refers to the use of sub-contractors by the monitoring body. The Board is of the opinion that, even when sub-contractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity. Although the Board identifies that the examples given in this subsection are in this direction, the Board recommends the NL SA to explicitly clarify this requirement in the draft accreditation requirements.
22. The Board observes that, according to subsection 1.3.3 of the NL SA's draft accreditation requirements, when using sub-contractors for processes relating to monitoring actions, evidence for demonstrating that the use of subcontractors does not remove or diminish the responsibility of the monitoring body may include "*written contacts or agreements to outline for example responsibilities, confidentiality, what type of data will be held and a requirement that the data is kept secure*", as well as a documented clear procedure for subcontracting. The Board encourages the NL SA to redraft the text in order to include requirements relating to the termination of those contracts, in particular so as to ensure that the subcontractors fulfil their data protection obligations.
23. The Board observes that subsection 1.4.1 under the section on "accountability" is more related to legal and decision making procedures (i.e. to section 1.1) than accountability. Therefore, the Board encourages the NL SA to make an appropriate amendment in the text.

2.2.3 EXPERTISE

24. Regarding the accreditation requirement in terms of the expertise of the monitoring body (section 2 in the NL SA's draft accreditation requirements), the Board acknowledges that the guidelines set a high bar requiring monitoring bodies to have an in-depth understanding of data protection issues.

Therefore, the Board encourages the NL SA to appropriately amend the relevant requirement in the subsection 2.2.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

25. The Board observes the NL SA's draft accreditation requirements refers twice to "the number of code members". More precisely, in the third paragraph in the 'explanatory notes' subsection of section 3 on established procedures and structures, the number of code members is being mentioned as a factor to be taken into account by the monitoring procedures. The Board also notes the same reference to 'number of code members' in requirements 3.2. Provided that the number of code members might not be known when the monitoring body applies for accreditation and that may change considerably after the accreditation has been granted, the Board recommends the NL SA to include, in both above places, appropriate references to "the expected number and size of code members", to align the text with the Guidelines and allow for more flexibility.
26. Moreover, in the same subsection, it is stated (last paragraph) that "*the monitoring body shall apply the penalties as defined in the code of conduct*". By only referring to penalties, the explanatory note seems to restrict the margin of manoeuvre of the monitoring body with regard to the kind of measures it can apply. The Board considers that a more comprehensive wording would also mention corrective measures, and encourages the NL SA to add the suggested reference in the explanatory note.
27. With regard to established procedures and structures (section 3 in the NL SA's draft accreditation requirements), the Board is of the opinion that the procedures to monitor compliance with codes of conduct have to be specific enough to ensure a consistent application of the obligations of code monitoring bodies. In particular, the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear timeframe, and check the eligibility of members prior to joining the code. Therefore, the Board recommends that the NL SA develop further these requirements and add examples of the above procedures (such as, procedures providing for audit plans to be carried out over a definite period and on the basis of predetermined criteria).

2.2.5 TRANSPARENT COMPLAINT HANDLING

28. With regard to the complaints handling procedure, the Board observes that the explanatory note (section 4 in the NL SA's draft accreditation requirements) states that "*personnel will demonstrate sufficient knowledge and impartiality*". The Board considers that the level of knowledge required to handle complaints would be better understood if the NL SA refers to "adequate knowledge" defining its meaning and therefore it encourages the NL SA to do so.
29. The Board notes that in the subsection 4.1 in the NL SA's draft accreditation requirements regarding complaints against code members, it is stated that "*the monitoring body shall provide evidence of a clear framework for a publicly available, accessible and easily understood complaints handling and decision-making process*". The Board encourages the NL SA to consider practical examples for the process of a complaints handling procedure, such as that the monitoring body should outline a procedure to receive, manage and process complaints, which in turn shall be publicly available and easily accessible.
30. The Board observes that in the subsection 4.4 in the NL SA's draft accreditation requirements it is stated that the monitoring body should inform the SA about the measures taken and justification of

any infringements leading to code member suspension or exclusion. However the Board recommends the NL SA to also include the notification to the code members and code owner as explicit requirements, in line with the Guidelines.

31. Regarding section 4.6 in the NL SA's draft accreditation requirements, the Board notes that the decisions of the monitoring body shall be made publicly available in line with its complaints handling procedure, whereas this information could include but is not limited to, general statistical information concerning the number and type of complaints/infringements and the resolutions/corrective measures issued and shall include information concerning any sanctions leading to suspensions or exclusions of code members. Without prejudice to national legislation, the Board encourages the NL SA to amend this requirement so that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate.

2.2.6 CONFLICT OF INTEREST

32. The Board takes note that in the NL SA's 'explanatory notes' section concerning the requirements for non-conflict of interest, some possible sources of risks to impartiality of the monitoring body are being described. However, the Board is of the opinion that, for practical reasons, more concrete examples of cases where a conflict of interest could arise might be helpful. An example of a conflict of interest situation would be the case where personnel conducting audits or making decisions on behalf of a monitoring body had previously worked for any of the organisations adhering to the code. In order to avoid any conflict of interest, the personnel would declare their interest and the work would be reallocated. Therefore, the Board encourages the NL SA to add some examples in the requirements.
33. The Board notes that in the Section 5.1 in the NL SA's draft accreditation requirements, it is stated that "*the monitoring body shall have in place a documented procedure to identify, analyse, evaluate, treat, monitor and document on an ongoing basis any risks to impartiality arising from its activities*". The Board recommends the NL SA, in line with the Guidelines, to amend this requirement so as to explicitly stress that the monitoring body shall refrain from any action incompatible with its tasks and duties.
34. The Board also notes that the monitoring body, according to the subsection 5.2 in the NL SA's draft accreditation requirements, shall choose or direct and manage its personnel. The Board is of the opinion that this requirement should be aligned with the Guidelines by explicitly adding the possibility that the staff can be provided by other body independent of the code. In this direction, some examples might also be helpful. An example of staff provided by a body independent of the code would be monitoring body personnel that have been recruited by an independent external company, which provides recruitment and human resources services. Therefore, the Board encourages the NL SA to appropriately amend this requirement.

2.2.7 REVIEW MECHANISMS

35. The Board observes that, in the subsection 7.1 in the NL SA's draft accreditation requirements, it is stated that "*the monitoring body will contribute to reviews of the code as required by the code owner and shall therefore ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members and continues to meet the application of the GDPR*". In line with the Guidelines, the review mechanisms should take into account any changes in the application and interpretation of the law or where there are new technological developments

which have impact upon the data processing carried out by the code members or the provisions of the code. Therefore, the Board encourages the NL SA to appropriately enrich this requirement.

2.2.8 LEGAL STATUS

36. With regard to the legal status of the monitoring body, the NL SA's explanatory note for this section states that the monitoring body "*must demonstrate sufficient financial and other resources to deliver its specific duties and responsibilities*". The Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time. Thereby, the Board encourages that the NL SA amend the explanatory note, adding the above-mentioned reference to "procedures".
37. Moreover, the code of conduct itself will need to demonstrate that the operation of the code's monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that a monitoring body demonstrates that it can deliver the code of conduct's monitoring mechanism over a suitable period of time. Therefore, the Board recommends NL SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.

3 CONCLUSIONS / RECOMMENDATIONS

38. The draft accreditation requirements of the NL Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
39. Regarding *general remarks* the Board recommends that the NL SA:
 1. Explicitly state that in case of substantial changes to the monitoring body relating to the monitoring body's ability to function independently and effectively, a review of the body to ensure that it still meets the requirements for accreditation will be always conducted.
40. Regarding *independence* the Board recommends that the NL SA:
 1. Redraft the explanatory note reference to 'requirements for independence' so that it is in line with the Guidelines, pointing out that the independence should be demonstrated in relation also to the profession, industry or sector to which the code applied, and put in the 'requirements' section;
 2. Clarify in the paragraph 1.1.2 that internal monitoring bodies can be set up only within a code owner.
 3. Add in section 1.3.3 that when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.
41. Regarding *conflict of interest* the Board recommends that the NL SA:
 1. To amend the requirement in Section 5.1 so as to explicitly stress that the monitoring body shall refrain from any action incompatible with its tasks and duties, in line with the Guidelines.
42. Regarding *established procedures and structures* the Board recommends that the NL SA:

1. Include appropriate references to “the expected number and size of code of code members” in the ‘explanatory notes’ subsection of section 3 and in the requirements 3.2, to align the text with the Guidelines and allow for more flexibility.
 2. Further develop under section 3 the procedures to monitor compliance with codes of conduct and includes examples of such procedures.
43. Regarding *transparent complaint handling* the Board recommends that the NL SA:
1. Include in the requirements 4.4 that information about the measures taken and justification of any infringements leading to code member suspension or exclusion should be additionally provided to the code members and code owner, in line with the Guidelines.
44. Regarding *legal status* the Board recommends that the NL SA:
1. Require that the monitoring body should demonstrate that it can deliver the code’s monitoring mechanism over a suitable period of time.

4 FINAL REMARKS

45. This opinion is addressed to the NL supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
46. According to Article 64 (7) and (8) GDPR, the NL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
47. The NL SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 19/2020 on the draft decision of the competent supervisory authority of Denmark regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 23 July 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the DK SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS	5
2.2.2	INDEPENDENCE	5
2.2.3	CONFLICT OF INTEREST	6
2.2.4	ESTABLISHED PROCEDURES AND STRUCTURES	6
2.2.5	COMMUNICATION WITH THE DK SA	7
2.2.6	LEGAL STATUS	7
3	CONCLUSIONS / RECOMMENDATIONS	7
4	FINAL REMARKS.....	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Danish Supervisory Authority (hereinafter "DK SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 27th May 2020.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the DK SA to take further action.
7. This opinion does not reflect upon items submitted by the DK SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the DK SA's accreditation requirements for Code of Conduct's monitoring bodies

8. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board encourages the DK SA to improve the layout and the format throughout the entire draft accreditation requirements submitted to the Board.
10. In addition, for the sake of clarity, the Board encourages the DK SA to explicitly refer at the first paragraph of the introduction of the draft accreditation requirements to the 01/2019 EDPB Guidelines with regard to the claim that a monitoring body is obligatory in a private sector Codes of Conduct.
11. The Board encourages the DK SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.

2.2.2 INDEPENDENCE

12. With regard to legal and decision-making procedures of the DK SA draft accreditation requirements (section 1.1), the Board acknowledges the impartiality of the monitoring body from the code members,

the profession, industry or sector to which the code applies. However, the Board is of the opinion that these requirements should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members. For this reason, the Board encourages the DK SA to amend this paragraph accordingly.

13. Regarding the internal monitoring bodies, the DK SA's draft accreditation requirements provides that the evidence of the monitoring body's independency may be demonstrated by "*a description of the operation of any committees, separate department or personnel that may be involved with the monitoring body*" (section 1.1.5 (h)). However the Board notices that such evidence may not suffice to demonstrate independence, taking into consideration the specific risks for independence that are raised in case of internal monitoring bodies. In view of the above, the Board encourages the DK SA to add more concrete examples of appropriate evidence, such as information barriers, separate reporting structures. The Board is aware of the fact that such examples of evidence are provided in the subsequent section 1.3.5 of the draft accreditation requirements. The Board encourages the DK SA to add such examples at the section 1.1.5 for reasons of clarity and consistency.
14. With regard to the financial independence of DK SA draft accreditation requirements (section 1.2), the Board considers that the financial independence should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. Such requirements include the number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the processing operation(s). Therefore, the Board encourages the DK SA to redraft the requirements accordingly.
15. With regard to monitoring body's responsibility for its decisions regarding the monitoring activities, the DK SA provided in its draft accreditation requirements (section 1.3.4) "*The personnel of the monitoring body can be held responsible for their activity in accordance with the Danish penal law*". The Board encourages the DK SA to refer in general to the Danish law instead of referring only to the penal law.

2.2.3 CONFLICT OF INTEREST

16. The Board recognizes that one of the biggest risks related to the monitoring body is the risk of impartiality. The Board notes that such risk may arise not only from providing services to the code members but also from a wide range of activities carried out by the monitoring body vis-à-vis code owners (especially in the situation where the monitoring body is an internal one) or other relevant bodies of the sector concerned. In this context, the Board encourages the DK SA to provide additional clarifications and examples of situations where there is not conflict of interest. Examples could include, among others, services, which are purely administrative or organisational assistance or support activities which have no influence on the impartiality of the monitoring body.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

17. With regard to the established procedures and structures, the EDPB notes that section 4.1 of the DK SA draft requirements provides that "*Resources should be proportionate to the expected size of code members, as well as the complexity of degree of risk of the relevant data processing and the expected received complaints*". The Board encourages the DK SA, in addition to the "*expected size of the code members*" to add the number of the code members as well for consistency with the section 4.8 of the draft accreditation requirements.

18. Regarding section 4.10 of DK SA's draft accreditation requirements, the Board notes that the monitoring body's decisions, or general information thereof, shall be made publicly available in line with its complaints handing procedure. Without prejudice to national legislation, the Board encourages the DK SA to amend this requirement so that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate. However, data subjects should, in any case, be informed about the status and outcome of their individual complaints, so that the transparency requirements of this procedure are respected.

2.2.5 COMMUNICATION WITH THE DK SA

19. With respect to the communication with the DK SA (section 6.1), it is stated that "*the monitoring body must set out clear reporting mechanisms to allow for reporting without undue delay of any repeated or serious infringements (which would result in severe actions such as suspensions or exclusion from the code) issued by the monitoring body to the Danish DPA*". The Board welcomes the fact that not all the complaint and not every single action, audit, review or investigation vis-à-vis code members is communicated to the DK SA, but only the serious cases. However, the Board recommends the DK SA to appropriately add a requirement regarding the reporting of non-serious cases. An example of such requirement could be that the monitoring body should be able to provide relevant information of its action upon DK SA's request.

2.2.6 LEGAL STATUS

20. According to section 8 of the DK SA's draft accreditation requirements "*the monitoring body must demonstrate that it has an appropriate standing to carry out its role under Article 41 (4) of the GDPR and that it is capable of being fined cf. Article 83 (4)(c) of the GDPR and Paragraph 41 (1)(3) of the Danish Data Protection Act ("Databeskyttelsesloven") and when relevant Paragraph 41 (6) of the Danish Data Protection Act.*". The Board is of the opinion that, financial capacity shall not prevent small or medium monitoring bodies from being accredited. It is enough to have a legal capability of being fined. Therefore the Board encourages the DK SA to either delete this requirement or to soften the wording and refer to the monitoring body's responsibilities in general and not put an emphasis on the fines.

3 CONCLUSIONS / RECOMMENDATIONS

The draft accreditation requirements of the DK Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:

21. Regarding *communication with the DK SA* the Board recommends that the DK SA:
1. amends section 6.1 so to reflect that not all the cases should be communicated to the DK SA.
The Board welcomes the fact that not all the complaint and not every single action, audit, review or investigation vis-à-vis code members is communicated to the DK SA, but only the serious cases. However, the DK SA should add a requirement regarding the reporting of non-serious cases.

4 FINAL REMARKS

22. This opinion is addressed to the Danish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
23. According to Article 64 (7) and (8) GDPR, the DK SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
24. The DK SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 20/2020 on the draft decision of the competent supervisory authority of Greece regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 23 July 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the EL SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS	5
2.2.2	INDEPENDENCE	7
2.2.3	CONFLICT OF INTEREST	8
2.2.4	EXPERTISE	9
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	9
2.2.6	TRANSPARENT COMPLAINT HANDLING	9
2.2.7	REVIEW MECHANISMS	10
2.2.8	LEGAL STATUS	10
3	CONCLUSIONS / RECOMMENDATIONS.....	10
4	FINAL REMARKS.....	11

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Hellenic Supervisory Authority (hereinafter "EL SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 28 May 2020.
2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

3. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
4. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements

foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

5. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
6. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
7. When this opinion remains silent on a specific requirement, it means that the Board is not asking the EL SA to take further action.
8. This opinion does not reflect upon items submitted by the EL SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the EL SA’s accreditation requirements for Code of Conduct’s monitoring bodies

9. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The Board is of the opinion that examples help in understanding draft requirements. Therefore, the Board encourages the EL SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some additional examples. In particular, the Board encourages EL SA to add:
 - examples of the information or documents that applicants have to submit when applying for accreditation;
 - examples of what may constitute an internal monitoring bodies (i.e. ad hoc internal committee or separate department within the organisation of the code owner; section 1 of the draft requirements);

- examples of data protection expertise (e.g. expertise may be demonstrated for example by submitting evidence of adequately trained educated and experienced staff in these domains, for example by means of a diploma, certification or a proof of experience; section 3 of the draft requirements);
 - examples of significant changes taking place in the body which lead to the need for reaccreditation (e.g. any change that impacts on the monitoring body's ability to perform its function independently and effectively or would be likely to call into question its independence, expertise and the absence of any conflict of interests or to adversely affect its full operation);
 - examples of the kind of information that the monitoring body is expected to include in the annual report (section 7a of the draft requirements);
 - examples of the different ways a monitoring body can be set up (i.e. a limited company, an association, an internal department within the code owner's organisation or as a natural person; section 8 of the draft requirements).
11. According to the Guidelines, codes are a mechanism which can be used to assist organisations in demonstrating their compliance with the GDPR (paragraph 10 of the Guidelines). In this context, it should be noted that specific rules and/or practices cannot ensure compliance with the overall conditions for lawful processing of personal data as set out in the GDPR. Therefore, the Board recommends to the EL to replace in the second paragraph of the introduction the phrase "ensure compliance" with "help ensuring compliance" or "assist organisations in demonstrating compliance".
12. In the third paragraph of the introduction, the Board encourages EL SA to include a reference to Art. 40.5 of the Regulation, this would allow to keep consistency with other paragraphs where references to relevant provisions of the GDPR are included. Also, in the Board's opinion an approved code of conduct can be used not as an evidence, but only as supporting evidence to demonstrate compliance with the obligations of the controller/ processor - the Board encourages EL SA to introduce relevant changes.
13. In paragraph nine of the introduction, the Board encourages EL SA to use the term "monitoring body" instead of body. Also phrase "associated with" shall be replaced with a sentence that the accreditation of a monitoring body applies only for a specific code, as indicated in the Guidelines (see definition of the accreditation).
14. As regards paragraph 10 of the draft requirements, the Board would like to underline that the accreditation requirements may be reassessed sooner than after 5 years. Therefore the Board encourages EL SA to clarify that the requirements may be reviewed periodically, also before the end of the 5 years period. Moreover, the Board notes that it is only the monitoring body that is allowed to submit a request for renewal to the supervisory authority. Therefore, the Board recommends to remove a reference to the code owner, when mentioning request for renewal in this paragraph.
15. In relation to the codes that are used as instruments for international transfers (paragraph 11 of the introduction), the Board recommends EL SA to delete the last part of the last sentence, i.e. "which will be considered in separate guidelines", as it refers to a future event.
16. With respect to basic definitions and the definition of a "code member" the Board encourages EL SA to remove a reference to adherence. If a controller or processor signed up to the code it also means that he adhered to the code and its obligations.

17. Finally, the Board encourages EL SA to ensure consistency in wording used, in particular regarding references to EL SA (HDPA and Authority are used interchangeably).

2.2.2 INDEPENDENCE

18. With respect to definition of independence, the Board encourages EL SA to elaborate what independence means. To ensure consistency such clarification could rely on the wording agreed by the Board in the previous opinions. According to the Board, independence for a monitoring body should be understood as a series of formal rules and procedures for the appointment, terms of reference and operation of the monitoring body. In Board's view these rules and procedures will allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced, nor subject to any form of pressure that might affect its decisions. This means that a monitoring body should not be in a position to receive any instructions regarding the exercise of its task from code members, the profession, industry or sector to which the code applies, or from the code owner itself.²
19. In Board's view, when the monitoring body is part of the code owner organisation, particular focus must be made on their ability to act independently. Rules and procedures have to be established to ensure that this committee acts autonomously and without any pressure from the code owner or the code members. Bearing the above in mind, with respect to organisational independence, the Board recommends EL SA to elaborate and better explain in the section 1 of the draft requirements what is the ability of a monitoring body to act independently.
20. The Board encourages, for the sake of consistency with previous opinions, to replace the headline "Legal independence in decision-making procedures" with "Legal and decision making procedures".
21. In section 1.i.A, the Board, taking into consideration the importance of the ability to act independently, encourages EL SA to replace "independent in making decisions" with a more broad term "independent in decision making procedures".
22. For the sake of consistency with previous opinions, in section 1.i.B the Board encourages EL SA to replace references to "people" with "personnel". Also, the Board encourages EL SA to be consistent in use of "shall/should/must". With respect to ensuring that the monitoring body shall neither receive nor take instructions/guidance from anyone, EL SA is encouraged to indicate that this requirement applies not only to the monitoring body but also to its personnel involved in decision-making process. As regards the example provided by EL SA and the reference to documents and recorded procedures currently applicable establishing its independence in decision making, the Board recommends deletion of the word "current" - in the opinion of the Board such documents and recorded procedures must be in place all the time.
23. As regards section 1.i.C and the internal monitoring body, the Board notes that the requirement that an internal monitoring body cannot be setup within a code member seems to be missing. Therefore, the Board recommends adding a relevant provision.

² See paragraph 14 of Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR.

24. The monitoring body must have sufficient financial and other resources together with the necessary procedures to ensure the functioning of the code of conduct over time. That is why, with respect to section 1.ii.A of the draft requirements, the Board recommends to clarify that long-term financing should be ensured.
25. With respect to section 1.iii.A, the Board encourages EL SA to explain what does “necessary” human resources mean. The Board encourages EL SA to consider making a reference to “sufficient numbers of sufficiently qualified personnel”. Also, the Board encourages EL SA to include a reference to technical resources necessary for the effective performance of monitoring body’s tasks.
26. As regards section 1.iii.C of the draft requirements, the use of sub-contractors implies that they will provide same guarantees and safeguards as the monitoring body. In this context, safeguards provided by sub-contractors cannot be proportionate but need to be the same as implemented by the monitoring body. Therefore, the Board recommend to delete a reference to “full proportion” in this section.

As regards the same section, the Board would like to point out that a monitoring body is always responsible for the decision-making and for the compliance with the code. With respect to who should prepare the final decision, there is no doubt that it should be made by the monitoring body, not a sub-contractor, therefore the Board recommends to EL SA to use “shall” instead of “should” when referring to the monitoring body making the final decision. Lastly, the Board encourages EL SA to explicitly indicate that obligations applicable to the monitoring body are applicable in the same way to the sub-contractor.

Finally, the Board is of the opinion that when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entities. The Board encourages EL SA to introduce a direct reference to effective monitoring.

2.2.3 CONFLICT OF INTEREST

27. As regards section 2 of the draft accreditation requirements, the Board agrees with EL SA that the monitoring body shall have in place clear procedures to ensure that no natural or legal person carrying out code compliance monitoring tasks is linked, directly or indirectly, to the code member under scrutiny in such a way which may yield a conflict of interest. At the same time, the Board is of the opinion that such links should also be prohibited not only for code member, but also for the code owner and encourages EL SA to add the relevant reference.

With respect to the same section, the Board underlines that monitoring body’s personnel shall be obliged to report any situation likely to create a conflict of interest. A clear indication that personnel does not have any situation which could compromise its impartiality in decision making could be of use. In this context, the Board encourages the EL SA to add examples which would clarify in a better way what situation could likely constitute a conflict of interest.

2.2.4 EXPERTISE

28. As regards section 3 of the draft requirements, the Board is of the opinion that the monitoring body not “should”, but, as it is obligatory, “shall” provide to the HDPA evidence that it has the expertise to undertake effective monitoring of a code. Also, the Board recommends to clarify what constitutes relevant qualifications (i.e. an in depth understanding and experience in relation to the specific data processing activities, appropriate data protection expertise and operational expertise) and to add a reference to relevant training, as an example.
29. The Board agrees with the EL SA, that expertise needs to involve the subject-matter (sector) of the code, in which case the relevant requirements that must be fulfilled can be specific, based on the sector to which the code applies. In this context, the Board recommends to clarify in section 3 that different interests involved and the risks of the processing activities addressed by the code should also be taken into account.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

30. With respect to section 4, the Board notes that it is mainly focussed on audits, however other ways to monitor controllers’ and processors’ compliance with the code should be included as well, for example review procedures, which can include such things as: audits, inspections, reporting and the use of self-monitoring reports or questionnaires. Also, the monitoring body shall demonstrate that it has a procedure for the investigation, identification and management of code member infringements to the code and additional controls to ensure appropriate action is taken to remedy such infringements as set out in the relevant code. In this context, the Board recommends to EL SA expanding this section to cover the above mentioned procedures.

As regards the same section, the Board underlines that the issue of the procedures to check for eligibility of members prior to joining the code is also of importance. The monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear time frame, and check eligibility of members prior to joining the code. Therefore, the Board recommends EL SA to reflect this in the text.

31. The Board recommends to EL SA to provide more information about what is approved policy and who approves it or when referring to “policy” in section 4, to delete the reference to “approved”.

2.2.6 TRANSPARENT COMPLAINT HANDLING

32. In order to provide for more clarity, as regards section 5.A.b of the draft requirements, the Board recommends replacing the sentence “[i]n the event that the body finds the complaint vague or unsubstantiated, this shall be substantiated” with “[t]he monitoring body shall contact the complainant in order to give the complainant the opportunity to further substantiate the complaint/fill in the missing information”.
33. With respect to section 5.A.e of the draft requirements, the Board, taking into account the importance of providing high level of transparency, recommends to EL SA to move the footnote to the main text.

- 34. In section 5.B.a of the draft requirements the Board encourages EL SA, for the sake of consistency, to replace the term “the person who submitted the complaint” with “complainant”.
- 35. With respect to section 6.b of the draft requirements, the Board encourages EL SA to specify who assess what constitutes a relevant evidence. Also, the Board encourages EL SA to specify that such evidence includes information outlining details of the infringement and actions taken.
- 36. As regards section 6.d of the draft requirements, for the sake of consistency, the Board recommends to replace the wording “significant change has occurred to the monitoring body” with “substantial changes in relation to the structure and functioning of the monitoring body have occurred”.

2.2.7 REVIEW MECHANISMS

- 37. As regards section 7, the Board is of the opinion that the monitoring body should be able to contribute to reviews of the code as required by the code owner and shall therefore ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members and continues to adapt to any changes in the application and interpretation of the law and new technological developments. Therefore, the Board recommends EL SA to reflect this in the text.

2.2.8 LEGAL STATUS

- 38. The Board would like to underline that accreditation of a monitoring body does not extend to an assessment of compliance with the Regulation. Therefore, in section 8 of the draft requirements, the Board encourages EL SA to clarify what does “presumption of recognition” mean.

3 CONCLUSIONS / RECOMMENDATIONS

- 39. The draft accreditation requirements of the Hellenic Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
- 40. Regarding *general remarks* the Board recommends that the EL SA:
 - 1. Replace in the second paragraph of the draft requirements the phrase “ensure compliance” with “help ensuring compliance” or “assist organisations in demonstrating compliance”.
 - 2. In paragraph 10 of the draft requirements, remove a reference to the code owner, when mentioning request for renewal.
 - 3. In paragraph 11 of the draft requirements, delete the last part of the last sentence, i.e. “which will be considered in separate guidelines”.
- 41. Regarding *independence* the Board recommends that the EL SA:
 - 1. Elaborate and better explain in section 1 of the draft requirements what is the ability of a monitoring body to act independently.
 - 2. In section 1.i.B of the draft requirements delete the word “current”.

3. In section 1.i.C of the draft requirements, add provision that an internal monitoring body cannot be setup within a code member.
 4. In section 1.ii.A of the draft requirements, clarify that long-term financing should be ensured.
 5. In section 1.iii.C of the draft requirements, delete a reference to “full proportion”.
 6. In section 1.iii.C of the draft requirements, use “shall” instead of “should” when referring to the monitoring body making the final decision.
42. Regarding *expertise* the Board recommends that the EL SA:
1. As regards section 3 of the draft requirements, clarify what constitutes relevant qualifications and that different interests involved and the risks of the processing activities addressed by the code should also be taken into account.
43. Regarding *established procedures and structures* the Board recommends that the EL SA:
1. With respect to section 4 of the draft requirements, expand it to cover different ways to monitor controllers’ and processors’ compliance with the code and to ensure appropriate action is taken to remedy possible infringements.
 2. As regards the same section, add reference to procedures to check for eligibility of members prior to joining the code and provide more information about what is approved policy and who approves it.
44. Regarding *transparent complaint handling* the Board recommends that the EL SA:
1. As regards section 5.A.b of the draft requirements, replace the sentence “[i]n the event that the body finds the complaint vague or unsubstantiated, this shall be substantiated” with “[t]he monitoring body shall contact the complainant in order to give the complainant the opportunity to further substantiate the complaint/fill in the missing information”.
 2. With respect to section 5.A.e of the draft requirements, move the footnote to the main text.
 3. As regards section 6.d of the draft requirements, for the sake of consistency, replace the wording “significant change has occurred to the monitoring body” with “substantial changes in relation to the structure and functioning of the monitoring body have occurred”.
45. Regarding *review mechanisms* the Board recommends that the EL SA:
1. As regards section 7 of the draft requirements, make a direct indication that the monitoring body should ensure that the code remains relevant to the members and continues to adapt to any changes in the application and interpretation of the law and new technological developments.

4 FINAL REMARKS

46. This opinion is addressed to the Hellenic Supervisory Authority and will be made public pursuant to Article 64 (5) (b) GDPR.
47. According to Article 64 (7) and (8) GDPR, the EL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision.

Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

48. The EL SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

61

Opinion of the Board (Art. 64)



Opinion 21/2020 on the draft decision of the competent supervisory authority of the Netherlands regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 23 July 2020

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	GENERAL REMARKS.....	6
2.2.2	GENERAL REQUIREMENTS FOR ACCREDITATION	6
2.2.3	RESOURCE REQUIREMENTS	7
2.2.4	PROCESS REQUIREMENTS.....	8
2.2.5	MANAGEMENT SYSTEM REQUIREMENTS.....	9
2.2.6	FURTHER ADDITIONAL REQUIREMENTS	9
3	Conclusions / Recommendations.....	9
4	Final Remarks	10

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Dutch supervisory authority (hereinafter “NL SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 28 May 2020. The NL national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the NL SA, once they are approved by the NL SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the NL SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.
3. This assessment of NL SA’s additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB’s

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the NL SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the NL SA to take further action.
8. This opinion does not reflect upon items submitted by the NL SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

9. Taking into account that:

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
- e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
- f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

10. The Board acknowledges that the NL SA's draft accreditation requirements include a section on terms and definitions. However, some of the terms are not used consistently throughout the document (e.g. "object of evaluation" and "ToE", the "accreditation body" and "RvA", the term "CB" is not used in the text, the text sometimes refers to "the competent supervisory authority" instead to the "NL SA"...). Additionally, the Board considers that, when referring to the ISO 17065, the relevant section should be mentioned. Whereas this is the case sometimes (e.g. sections 7.3, 7.5, 7.6, 7.7 and 7.9 of the NL SA's draft requirements), it is not consistent throughout the document (e.g. sections 4.2, 4.3, 4.6, 6.2, 7.1, 7.2, 7.4 and 7.8 of the NL SA's draft requirements do not mention the relevant sections of ISO 17065). The Board encourages the NL SA to ensure that the terms used are consistent and that the references to the ISO 17065 are clear.
11. The Board notes that some sections of the Annex are missing (e.g. section 9.3.2 of the Annex "Documentation of evaluation activities"). The Board understands that, in those cases, no additional requirements were formulated. However, for the sake of clarity, the Board encourages the NL SA to either add the missing sections or include a statement at the beginning of the draft requirements, clarifying that, when some sections are missing, it means that no additional requirements were formulated.

2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

12. The Board notes that the last paragraph of subsection 4.1.1 of the NL SA's draft accreditation requirements ("Legal responsibility") refer to investigations or regulatory actions "in relation to the subject matter of the ToE which may mean they do not meet this requirement and therefore might prevent their accreditation." The Board considers that the reference to the subject matter of the ToE

is not entirely correct in this case, since the requirement is related to the accreditation of the certification bodies and not to their certification activities. Therefore, the Board encourages the NL SA to delete the said reference in the last part of the requirement.

13. With regard to subsection 4.1.2 of the NL SA's draft accreditation requirements ("Certification agreement"), the Board notes that point 6 does not include all the elements of point 8 of the Annex. In particular, "the necessary precautions for the investigation of complaints" are missing. The Board recommends the NL SA to include the missing information from the Annex.
14. Additionally, the Board is of the opinion that point 7 of subsection 4.1.2 regarding the obligation of the applicant to inform the certification body of relevant infringements of the GDPR or the UAVG should be clarified. The Board considers that this obligation should not lead to self-incrimination and, therefore, the obligation should refer to infringements established by the NL SA and/or judicial authorities. Thus, the Board recommends the NL SA make such clarification. Moreover, in order to avoid confusion, the Board encourages the NL SA to clarify that "relevant infringements" refer to infringements of the GDPR or the UAVG that may affect certification.
15. Regarding point 9 of subsection 4.1.2, the Board notes the inclusion of a reference to the consequences for the data subjects. However, the NL SA omitted a reference to [where applicable] "the consequences for the customer should also be addressed", as stated in the Annex. The Board therefore recommends the NL SA to replace the term with "customer", in order to align the wording with the Annex.
16. With regard to section 4.3 ("Liability and financing") of the NL SA's draft accreditation requirements, the Board notes that, in accordance with the Annex, the certification body shall demonstrate on a regular basis that it has the appropriate measures to cover its liabilities. The NL SA's draft accreditation requirements do not include the notion of "regular basis" and, therefore, the Board recommends the NL SA to include such reference, in line with the Annex.
17. The Board notes that section 4.3 of the NL SA's draft accreditation requirements contains the obligation to having adequate financial resources to demonstrate how the fines, that may be imposed under article 83(4)(b) GDPR, will be paid. The Board considers that this specific reference to the fines under GDPR may lead to some difficulties in practice, especially with regard to the assessment of compliance with the requirements. Thus, the Board encourages the NL SA to reconsider the specific reference to fines under GDPR, taking into account the potential practical difficulties that such reference may imply.
18. The Board notes that section 4.6 of the NL SA's draft accreditation requirements ("Publicly available information") includes the obligation to demonstrate the publication of the approved criteria and "high-level explanations about the certification procedures". The Board notes that a "high-level" explanation may not be enough to provide the information required in the Annex. Therefore, the Board encourages the NL SA to add that "meaningful" explanations will be provided.

2.2.3 RESOURCE REQUIREMENTS

19. Concerning certification body personnel (section 6.1 of the NL SA'S draft accreditation requirements), the Board notes that the requirements follow the Annex. In this respect, the Board is of the Opinion that, with regard to the expertise of the certification body, the emphasis should be put on the different type of substantive expertise and experience. Specifically, the Board considers that the competence requirements for evaluators and decision-makers should be tailored taking into account the different

tasks that they perform. In the Board's opinion, evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the NL SA to redraft this section taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.

20. Additionally, the Board notes that, with regard to personnel with legal expertise, the Annex requires a specific educational background or significant professional experience. This last reference is missing in the NL SA's draft accreditation requirements. The Board recommends the NL SA to add such reference.
21. Moreover, regarding the educational requirements for personnel with technical expertise, the Annex refers to "a qualification in a relevant area of technical expertise to at least EQF level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession". The Board notes that the NL SA's draft accreditation requirements do not include the reference to a recognised protected title in the relevant regulated profession and recommends the NL SA to include such reference.

2.2.4 PROCESS REQUIREMENTS

22. Regarding section 7.2 ("Application") of the NL SA's draft accreditation requirements, the Board notes that point 4 includes the obligation to "*disclose any current or recent AP investigation or regulatory action to which the applicant is subject*". The Board is of the opinion that the obligation should be tailored to investigations or regulatory actions related to the scope of the certification and the target of evaluation. Therefore, the Board encourages the NL SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.
23. With regard to section 7.4 ("Evaluation"), point 3, the Board considers that the reference to the requirements "as set out in the criteria" seems to presuppose that the criteria are complete. While acknowledging that the NL SA has used the wording of the Annex, the Board encourages the NL SA to refer to "the adopted criteria", in order to avoid confusion.
24. The Board notes that the second paragraph of section 7.6 of the NL SA's draft accreditation requirements ("certification decision") includes the obligation to submit the draft approval to the NL SA, prior to issuing or renewing certification. Based on the explanations provided by the NL SA, the Board understand that the intention of this requirement is to increase transparency and it does not entail a supervision of the draft approval. The Board encourages the NL SA to include a clarification in that sense.
25. With regard to section 7.10 of the NL SA's draft accreditation requirements ("Changes affecting certification"), the Board notes that the first bullet point includes "any personal data breach or infringement of the GDPR". The Board considers that, in order to avoid self-incrimination, the reference should be to infringements established by the NL SA or the competent judicial authority. Additionally, the reference to "any data breach" seems quite broad. The Board is of the view that such reference should be further developed, in order to clarify whether minor data breaches should also be reported. Therefore, the Board encourages the NL SA to change the wording, by referring to "established" infringements and clarify the meaning of "any data breach".

- 26. The Board notes that the first sentence of section 7.11 is not formulated as a mandatory requirement. The Board encourages the NL SA to replace the word “should” by “shall”, to make clear that it is an obligation. Additionally, the Board notes that the obligation to inform about measures taken is also towards the NAB, as stated in the Annex. The Board recommends the NL SA to add such reference to the NAB.
- 27. Finally, section 7.13 of the NL SA’s draft accreditation requirements (“Complaints and appeals”), states the obligation to inform the complainant of the progress and the outcome of the complaint within one month of receipt of the complaint. Whereas transparency towards complainants is of great importance, the Board considers that a strict obligation to provide the complainant the outcome of the complaint in one month may create unrealistic expectations and pose a high challenge for the certification body. Therefore, the Board encourages the NL SA to redraft the requirements by stating that the certification body has to inform the complainants of the progress or the outcome within one month of receipt of the complaint.

2.2.5 MANAGEMENT SYSTEM REQUIREMENTS

- 28. With regard to section 8 of the NL SA’s draft accreditation requirements (“Management system requirements”), the Board notes that the obligation of the certification body to disclose to the NL SA the management principles and their documented implementation during the accreditation procedure is not foreseen. The Board recommends the NL SA to amend the draft requirements, by including such obligation, as stated in the Annex.

2.2.6 FURTHER ADDITIONAL REQUIREMENTS

- 29. Section 9.3.2 of the NL SA’s draft accreditation requirements (“Management of complaint handling”) does not include the obligation to share with the NL SA relevant complaints and objections, as stated in the Annex. The Board recommends the NL SA to include such obligation.

3 CONCLUSIONS / RECOMMENDATIONS

- 30. The draft accreditation requirements of the Dutch Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
- 31. Regarding ‘general requirements for accreditation’, the Board recommends that the NL SA:
 - 1) add the missing information from the Annex references in point 6 of subsection 4.1.2.
 - 2) clarify in point 7 of subsection 4.1.2 that the the obligation of the applicant to inform the certification body of relevant infringements of the GDPR or the UAVG should refer to infringements established by the NL SA and/or judicial authorities.
 - 3) replace in point 9 of subsection 4.1.2 the term with “customer”, in order to align the wording with the Annex.
 - 4) include in section 4.3 the reference to the notion of “regular basis”, in line with the Annex.
- 32. Regarding ‘resource requirements’, the Board recommends that the NL SA:

- 1) add in section 6.1 the reference to significant professional experience with regard to personnel with legal expertise
 - 2) add, in the educational requirements for personnel with technical expertise, a reference to a recognised protected title in the relevant regulated profession.
33. Regarding 'process requirements', the Board recommends that the NL SA:
- 1) add in section 7.11 the obligation to inform the NAB about measures taken, in line with the Annex.
34. Regarding 'management system requirements', the Board recommends that the NL SA:
- 1) include in section 8 the obligation to disclose to the NL SA the management principles and their documented implementation during the accreditation procedure.
35. Regarding 'further additional requirements', the Board recommends that the NL SA:
- 1) include in subsection 9.3.2 the obligation to share with the NL SA relevant complaints and objections, as stated in the Annex

4 FINAL REMARKS

36. This opinion is addressed to the Dutch Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
37. According to Article 64 (7) and (8) GDPR, the NL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
38. The NL SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 22/2020 on the draft decision of the competent supervisory authority of Greece regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 23 July 2020

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX	6
2.2.2	TERMS AND DEFINITIONS	7
2.2.3	GENERAL REMARKS.....	7
2.2.4	GENERAL REQUIREMENTS FOR ACCREDITATION	7
2.2.5	STRUCTURAL REQUIREMENTS	8
2.2.6	RESOURCE REQUIREMENTS	8
2.2.7	PROCESS REQUIREMENTS.....	9
2.2.8	FURTHER ADDITIONAL REQUIREMENTS	10
3	Conclusions / Recommendations.....	10
4	Final Remarks	10

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The “Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)” (hereinafter the “Guidelines”), and “Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679” will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

limited to, the requirements detailed in Article 43 (2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43 (1)(b). The EDPB notes that Article 43 (2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Hellenic Supervisory Authority (hereinafter “EL SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 28 May 2020. The Greek national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the EL SA, once they are approved by the EL SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the EL SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.]

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

3. This assessment of EL SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the EL SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the EL SA to take further action.
8. This opinion does not reflect upon items submitted by the EL SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

9. Taking into account that:

adopted

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
- e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
- f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

2.2.1 PREFIX

- 10. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.
- 11. The Board notes that the first point in section 0 of the EL SA's draft accreditation requirements states that "*In particular, the E.SY.D. shall provide the HDPA with a brief description of the request, the name and contact details of the certification body, the certification scheme for which accreditation is requested and whether the certification criteria are approved by the competent supervisory authority or the EDPB, or if their approval is pending.*" Based on the explanations provided by the EL SA, the Board understands that the last part of the sentence refers to those situations in which the accreditation application is submitted to the NAB before the certification criteria receive the final approval, but the accreditation will not be given until such approval takes place. In order to avoid confusion, the Board encourages the EL SA to clarify that the accreditation will not be granted until the certification criteria receive the final approval.
- 12. The Board notes that section 0 of the EL SA's draft accreditation requirements states that "*The HDPA, if it deems appropriate, shall inform the E.SY.D. within a reasonable time of any important reasons for non-compliance by the certification body with the GDPR. Although the E.SY.D. can continue the accreditation process, it shall not conclude it until the HDPA has reached its final decision in this respect.*" The Board encourages the EL SA to clarify that the NAB should take into account the decision

taken by the EL SA, although the NAB is free to decide with regard to the granting of accreditation, without prejudice to the power of the EL SA to revoke it afterwards, if appropriate.

2.2.2 TERMS AND DEFINITIONS

13. The Board notes that the reference to the guidelines on accreditation as “WP 261” is not updated. The EDPB adopted the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). Therefore, the Board encourages the EL SA to amend the wording and refer to the Guidelines 4/2018.

2.2.3 GENERAL REMARKS

14. The Board notes that some terms are not used consistently (e.g. reference to “competent SA” instead to the “EL SA” in some requirements, such as point 3 of subsection 4.1.2). Additionally, the Board considers that, when referring to a specific section of the ISO 17065 or Article of the GDPR, it should be clear to which of the two the reference is made (e.g. point 8 of subsection 4.1.2 does not make the distinction between the two different references). The Board encourages the EL SA to ensure that the terms used are consistent and that the references to the ISO 17065 and the GDPR are clear.

2.2.4 GENERAL REQUIREMENTS FOR ACCREDITATION

15. The Board notes that section 4.1.1 (legal responsibility) second indent (starting with “Inform the ESYD...”) and section 4.1.2 (certification agreement) point 11 of the EL SA’s accreditation requirements refer to the obligation to inform about “any infringements” of the GDPR. The Board is of the opinion that such obligation should not lead to self-incrimination and, therefore, the obligation should refer to infringements established by the EL SA and/or judicial authorities. Thus, the Board recommends the EL SA make such clarification.
16. With regard to section 4.1.2 (certification agreement) of the EL SA’s draft accreditation requirements, the Board notes that the first paragraph states that the certification agreement shall be “in writing”. In order to ensure that electronic certification agreements are also covered, the EDPB encourages the EL SA to replace “in writing” by “in written form” or equivalent wording.
17. Moreover, with regard to point 9 of section 4.1.2 of the EL SA’s draft accreditation requirements, the Board acknowledges the inclusion of appropriate procedures “into the management of the certification body”. The Board understands that the reference is to the management system and encourages the EL SA to clarify it accordingly.
18. Regarding section 4.1.3 of the EL SA’s draft accreditation requirements, the Board acknowledges the obligation to inform the EL SA about the data protection seals and marks and provide a copy. However, the Board is of the opinion that the addressees of such obligation are not clear from the requirement. Therefore, the Board encourages the EL SA to clarify the addressees of the above-mentioned obligation.
19. With regard to the requirements to manage impartiality (section 4.2 of the EL SA’s draft accreditation requirements) and, in particular, the reference to the conflict of interests in the last paragraph, the Board considers that the wording should be clarified. The Board acknowledges the importance to have requirements that ensure, firstly, that there are no conflicts of interests and, secondly, in the case that conflicts of interest are identified, that the certification body manages them. The Board is of the

opinion that the wording of the EL SA's draft requirements seems to reverse this logical order. In order to avoid confusion, the Board encourages the EL SA to rephrase the sentence by stating first that the certification body shall ensure that there are no conflicts of interest.

20. The Board notes that indent 2 of section 4.2 of the EL SA's draft accreditation requirements states that the certification body shall not be "affiliated" with the customer it assesses. The Board encourages the EL SA to clarify the wording, in order to reflect the independence of the certification body. For example, the EL SA could state that the certification body should not belong to the same company group nor should be controlled in any way by the customer it assesses.

2.2.5 STRUCTURAL REQUIREMENTS

21. The Board observes that section 5.1 of the EL SA' draft accreditation requirements make reference to the appointment of "a person with significant experience in the protection of personal data with responsibility for overseeing data protection compliance." The functions of this figure seem similar to those of a data protection officer. The Board encourages the EL SA to clearly set out the functions of this figure.

2.2.6 RESOURCE REQUIREMENTS

22. Concerning certification body personnel (section 6.1), the Board notes that the requirements follow the Annex. In this respect, the Board is of the Opinion that, with regard to the expertise of the certification body, the emphasis should be put on the different type of substantive expertise and experience. Specifically, the Board considers that the competence requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In the Board's opinion, evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the EL SA to redraft this section taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.
23. Additionally, regarding the educational requirements of the technical personnel, the Board considers that the list of subjects is already tailored to the technical expertise required by the Annex. Therefore, the Board encourages the EL SA to delete the reference to "natural sciences" from the list of subjects regarding the educational requirements of the technical personnel.
24. Finally, the Board considers that the last paragraph of section 6.1 is applicable to both personnel with technical expertise and with legal expertise. The Board encourages the EL SA to clarify that it includes both.
25. Regarding the educational requirements for personnel with technical expertise, the Annex refers to "a qualification in a relevant area of technical expertise to at least EQF level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession". However, there is no reference to the underlined sentence in the EL SA's draft accreditation requirements. Additionally, the reference to the qualification to at least EQF level 6 has been replaced by an explicit reference to a university degree. Taking into account the variety in the educational systems, the Board recommends that the EL SA's draft requirements be aligned with the wording of the Annex, taking into account the specific educational system and requirements established in national law. For example, the requirements

could refer to a qualification “in information technology, computer science or mathematics of at least EQF level 6 or an equivalent vocational education enjoying a recognised protected title in the Member State where it was issued”.

2.2.7 PROCESS REQUIREMENTS

26. The Board notes that section 7.2 of the EL SA’s draft accreditation requirements (“application”) contains a reference to the controller/processor contract(s) and their specific arrangements. While acknowledging that the EL SA has used the wording of the Annex, the Board encourages the EL SA to include a reference to joint controllers and their specific arrangements.
27. With regard to section 7.4 (“Evaluation”), point 3, the Board considers that the reference to the requirements “as set out in the criteria” seems to presuppose that the criteria are complete. While acknowledging that the EL SA has used the wording of the Annex, the Board encourages the EL SA to refer to “the adopted criteria”, in order to avoid confusion.
28. With regard to section 7.8 of the EL SA’s draft accreditation requirements (“directory of certified products”), the Board notes that the two paragraphs listing the information that shall be made publicly available seem to overlap, since the relationship between the two documents mentioned (directory and evaluation report) is not clear. The Board encourages the EL SA to clarify the relationship between the two documents mentioned in those paragraphs.
29. Regarding section 7.9 (“Surveillance”) of the EL SA’s draft accreditation requirements, the Board notes that the periodicity of the surveillance is stated as “at least twice during the certification cycle”. The Board considers that, when determining the periodicity of the surveillance, the risk associated with the processing should be taken into account. Therefore, the Board encourages the EL SA to include a risk-based approach with regard to the arrangements for surveillance.
30. Regarding section 7.11 of the EL SA’s draft accreditation requirements (“Termination, reduction, suspension or withdrawal of certification), the Board notes that the third paragraph states that, with regard to the obligation to accept the decisions and orders of the EL SA to not issue certification when the requirements for certification are no longer met, *“the certification body shall provide clear and documented evidence to the HDPA that the certification criteria are not being met”*. Based on further explanations provided by the EL SA, the Board understands that the obligation of the certification body is to provide evidence to the EL SA that proper action has been taken. The Board encourages the EL SA to clarify the meaning in those lines.
31. Additionally, the Board notes and welcomes the inclusion of a requirement related to serious data breaches. However, in order to avoid confusion, the Board encourages the EL SA to clarify that such requirement do not affect the obligation of the clients to inform the SA in accordance to the GDPR.
32. Finally, the Board notes that section 7.12 (“Records”) of the EL SA’s draft accreditation requirements includes the obligation to record the contact details of certification body personnel responsible for evaluation and certification decisions, and to make such information available to the EL SA upon request. The Board is of the opinion that the ultimate responsible for the activities of the certification body’s personnel is the certification body. Therefore, the Board encourages the EL SA to specify the purpose of the requirement.

2.2.8 FURTHER ADDITIONAL REQUIREMENTS

33. Regarding subsection 9.3.1 (“Communication between CB and its clients”), the Board notes that the EL SA’s draft accreditation requirements include the obligation to have procedures in place for implementing appropriate procedures and communication structures between the certification body and its clients. In section 3 (“Terms and definitions”) of the EL SA’s draft accreditation requirements, “client” is described as “the controller of processor that has been certified”. However, the requirements in subsection 9.3.1 of the EL SA’s draft accreditation requirements are also relevant for applicants and, therefore, the Board encourages the EL SA to clarify it.
34. The Board notes that the last paragraph of subsection 9.3.3 is not formulated as a mandatory requirement. The Board encourages the EL SA to replace the word “should” by “shall”, to make clear that it is an obligation. Additionally, the Board considers that relevant complaints and objections not only have to be notified to the EL SA, but they have to be shared with the EL SA. The obligation to share with the EL SA the relevant complaints and objections shall be clear in the requirements. Therefore, the Board recommends the EL SA to redraft the requirement by stating that relevant complaints and objections shall be shared with the EL SA.

3 CONCLUSIONS / RECOMMENDATIONS

35. The draft accreditation requirements of the Hellenic Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
36. Regarding ‘general requirements for accreditation’, the Board recommends that the EL SA:
 - 1) clarify in sections 4.1.1 and 4.1.2 that the obligation to inform about any infringements of the GDPR refers to infringements established by the EL SA and/or judicial authorities.
37. Regarding ‘resource requirements’, the Board recommends that the EL SA:
 - 1) align the wording regarding the education requirements for personnel with technical expertise with the Annex, taking into account the specific educational system and requirements established in national law.
38. Regarding ‘further additional requirements’, the Board recommends that the EL SA:
 - 1) redraft the requirement in subsection 9.3.3 by stating that relevant complaints and objections shall be shared with the EL SA.

4 FINAL REMARKS

39. This opinion is addressed to the Hellenic Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
40. According to Article 64 (7) and (8) GDPR, the EL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

41. The EL SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 23/2020 on the draft decision of the competent supervisory authority of Italy regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 23 July 2020

Table of contents

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the EDPB regarding the submitted draft decision	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	TERMS AND DEFINITIONS	6
2.2.2	GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements).....	6
2.2.3	RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)	7
2.2.4	PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements)	7
2.2.5	MANAGEMENT SYSTEM REQUIREMENTS (section 8 of the draft accreditation requirements).....	7
3	Conclusions / Recommendations.....	8
4	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43 (2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43 (1)(b). The EDPB notes that Article 43 (2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Italian Supervisory Authority (hereinafter “IT SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 27 May 2020. The Italian national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the IT SA, once they are approved by the IT SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43 (1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the IT SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

3. This assessment of IT SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the IT SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the IT SA to take further action.
8. This opinion does not reflect upon items submitted by the IT SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
 - b. independence of the certification body
 - c. conflicts of interests of the certification body
 - d. expertise of the certification body
 - e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
 - f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
 - g. transparent handling of complaints about infringements of the certification.
9. Taking into account that:

adopted

- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
- b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
- c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
- d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
- e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
- f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

2.2.1 TERMS AND DEFINITIONS

10. The Board notes that, in '3 Terms and definitions', the IT SA defines 'Client' as "the data controller or data processor applying for certification". This deviates from ISO 17065, which states that whenever the term "client" is used, it applies to both the "applicant" (seeking certification) and the "client" (that has been certified). It also deviates from Annex 1 the guidelines on accreditation, which differentiates between "applicant" and "client". The Board encourages the IT SA to delete the definition of "client", and to either use the terms "applicant" and "client" as they are used in Annex 1 of the guidelines on accreditation or to use "client" as it is used in ISO 17065. If the IT SA chooses to do the latter, the Board encourages the IT SA to add a note that "client" is being used in this manner.

2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements)

11. With regard to clause 7 of subsection 4.1.2 of the IT SA's draft accreditation requirements, the Board considers that the wording is slightly unclear with regard to whom the reasons for approving certification are provided. Therefore, the Board encourages the IT SA to redraft it in a way that provides more clarity.
12. With regard to subsection 4.3, the Board notes that the draft additional accreditation requirements require the certification body to "confirm [...] it complies with the payment of pension contributions and other allowances; it is not the subject of tax injunction orders [...]" . The Board encourages the IT SA to clarify why these obligations, which are unrelated to the GDPR, are included in the draft additional accreditation requirements.

2.2.3 RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)

13. The Board notes that, in subsection 6.1, the draft additional accreditation requirements of the IT SA mostly follows the wording given in Annex 1 of the guidelines on accreditation. However, where Annex 1 states that certification personnel shall be “registered as applicable” this is omitted in the IT draft additional requirements. The Board recommends that the IT SA either reinstates the wording about certification personnel being “registered as applicable”, or clarifies that there is no obligation for registration under IT law.
14. The Board notes that in subsection 6.1, among the eligibility requirements for personnel responsible for certification decisions, it is stated that they “shall not be or have been struck off the respective professional registers on account of disciplinary reasons or any other grounds”. The Board encourages the IT SA to clarify why having been struck off the professional register on other grounds than disciplinary actions would lead to ineligibility.
15. The Board notes that, among the eligibility requirements for personnel responsible for certification decisions, it is stated that they “shall not be or have been the subject of measures restricting personal freedom”. The Board encourages the IT SA to clarify what is meant by “measures restricting personal freedom”.

2.2.4 PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements)

16. With regard to subsection 7.4 of the draft additional accreditation requirements, the Board encourages the IT SA to clarify the paragraph on pre-existing certification by replacing “previous certification activity” by “existing certification” and by clarifying what is meant by “the object of the latter”.
17. In the paragraph starting with “in addition to item 7.4.6 of ISO 17065”, the Board notes the wording “the CB shall set out in detail in its certification process...”. The Board encourages the IT SA to add that the CB shall set this out in a written document which could be either the certification scheme or, if the CB isn’t the scheme owner, another document pertaining to the certification process.
18. With regard to subsection 7.10 of the IT SA’s additional accreditation requirements, the Board considers that changes in the state of art are relevant and might affect certification. Therefore, the Board encourages the IT SA to include this possibility among the list of changes that might affect certification.

2.2.5 MANAGEMENT SYSTEM REQUIREMENTS (section 8 of the draft accreditation requirements)

19. In Annex 1 of the guidelines on accreditation, chapter 8 starts with subsection “8.1 General management system requirements”. In ISO 17065, chapter 8 starts with subsection “8.1 Options”. In their draft requirements, the IT SA also uses “8.1 Options”. To maintain the consistency with Annex 1, and in order to avoid misinterpretation by providing a clear and unambiguous reference to ISO 17065, the Board encourages the IT SA to change the title of subsection 8.1 to “8.1 General management system requirements”, and to refer to subsection 8.1 in ISO 17065 by its full title, i.e. “No additional requirements are laid down to 8.1 Options of ISO/IEC 17065:2012”.

3 CONCLUSIONS / RECOMMENDATIONS

20. The draft accreditation requirements of the IT Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
21. Regarding ‘resource requirements’, the Board recommends that the IT SA:
 - 1) either reinstates the wording from Annex 1 about certification personnel being ‘registered as applicable’, or clarifies that there is no obligation for registration under IT law.

4 FINAL REMARKS

22. This opinion is addressed to the Italian Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
23. According to Article 64 (7) and (8) GDPR, the IT SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
24. The IT SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 28/2020 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of Iberdrola Group

Adopted on 8 December 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Iberdrola Group were reviewed by Spanish Supervisory Authority (Agencia Española de Protección de Datos) as the lead supervisory authority (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Iberdrola Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 25 September 2020. The decision on the completeness of the file was taken on 9 October 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Iberdrola Group cover processing of personal data transferred, directly or indirectly, from a group company established in the EEA to a group company not established in an EEA country, including the initial transfers as well as onward transfers.
4. Concerned data subjects include candidates, employees, suppliers, volunteers, event attendees and participants in master's degree scholarships competitions and beneficiaries thereof.
5. The draft BCR-C of Iberdrola Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Iberdrola Group draft BCR-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Iberdrola Group Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Iberdrola Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁶, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁶ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

Opinion of the Board (Art. 64)



Opinion 29/2020 on the draft decision of the Lower Saxony Supervisory Authority regarding the Controller Binding Corporate Rules of Novelis Group

Adopted on 8 December 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Novelis Group were reviewed by the Lower Saxony Supervisory Authority as the - Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Novelis Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 24/09/2020. The decision on the completeness of the file was taken on 13/10/2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Novelis Group applies to the transfers and processing of personal data from EU to third countries carried out by Novelis Group companies.⁶
4. Concerned data subjects include current and former employees, job applicants, customers, suppliers, contractors and contact persons.
5. The draft BCR-C of Novelis Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Novelis Group draft BCRs-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Binding Corporate Rules for Novelis Group, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Novelis contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁶ As "Novelis Group" as defined in section 2.2 of Novelis Group BCR-C.

⁷ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 32/2020 on the draft decision
of the Dutch Supervisory Authority regarding
the Controller Binding Corporate Rules of Equinix**

Adopted on 15 December 2020

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Having regard to EDPB [Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc.](#), adopted on 8 October 2019.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. On 8 October 2019 the EDPB adopted its [opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc.](#) On 22 July 2020, the EDPB adopted an information note on BCRs for Groups of undertakings / enterprises

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

which have ICO as BCR Lead SA, which explained that for BCRs already approved under the GDPR, the new BCR Lead SA in the EEA, as the new competent Supervisory Authority (“SA”) in accordance with Article 47.1 GDPR, will have to issue a new approval decision following an opinion from the EDPB before the end of the transition period. The Dutch Supervisory Authority has taken over the role as Lead SA.

2. In accordance with the cooperation procedure as set out in WP263 rev.01, the proposed revisions to the BCR-C of Equinix were reviewed by the Dutch Supervisory Authority as the Lead SA (hereinafter the “BCR Lead SA”).
3. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Equinix, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 3 December 2020. The decision on the completeness of the file was taken on 3 December 2020.

2 ASSESSMENT

4. The BCRs of Equinix, contained in the Global Privacy Policy and its Appendices, cover personal data transferred from entities of Equinix Inc. in the EEA to entities of the group outside the EEA and processed by those entities outside the EEA.
5. Concerned data subjects include employees and business contacts, i.e. suppliers and vendors.
6. The revisions proposed to the BCR-C of Equinix have been scrutinised according to the procedures set up by the EDPB in light of the '*Checklist of elements for Controller and Processor BCRs which need to be amended for a BCR Lead SA change in the context of Brexit*'⁶.
7. Beyond those provisions in need of revision according to the checklist, the EDPB recalls its Opinion 15/2019 on the draft decision of the competent supervisory authority of the United Kingdom regarding the Binding Corporate Rules of Equinix Inc., adopted on 8 October 2019.
8. In light of the above, the EDPB does not have any concerns that need to be addressed with respect to the draft decision of the Dutch SA.

3 CONCLUSIONS / RECOMMENDATIONS

9. Taking into account the above and the commitments that the group members undertake by signing the Equinix Intra-Company Agreement on Binding Corporate Rules , the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Equinix contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

⁶ Annex to the EDPB information note on BCRs for Groups of undertakings / enterprises which have ICO as BCR Lead SA, adopted on 22 July 2020. https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-bcrs-groups-undertakings-enterprises-which-have_en

4 FINAL REMARKS

10. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
11. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
12. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
13. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

Opinion of the Board (Art. 64)



Opinion 1/2021 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Saxo Bank Group

Adopted on 22 January 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Saxo Bank Group were reviewed by the Danish Supervisory Authority (Danish Data Protection Agency – Datatilsynet) as the - Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Saxo Bank Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 9 November 2020. The decision on the completeness of the file was taken on 26 November 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Saxo Bank Group cover all the processing of personal data conducted by all entities of Saxo Bank Group.⁶
4. Concerned data subjects include potential, existing and former employees, clients, partners and vendors.
5. The draft BCR-C of Saxo Bank Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Saxo Bank Group draft BCRs-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by taking the steps to be bound by the BCRs, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs-C of Saxo Bank Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Danish Supervisory BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Danish Supervisory BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁶ As defined under section 2 of Saxo Bank Group BCRs.

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 2/2021 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of Elanders Group

Adopted on 22 January 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Elanders Group were reviewed by the Swedish Supervisory Authority as the Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Elanders Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 17 November 2020. The decision on the completeness of the file was taken on 26 November 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Elanders Group covers all processing of personal data relating to data subjects by all Elanders Group companies and those who are obligated to these BCR by contract having their headquarter: 1) outside an EEA country to the extent that this personal data has been transferred from a participating company established in an EEA country or established in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission to a participating company established outside the EEA; and 2) in an EEA country or in a country with an adequate level of data protection as acknowledged by a decision of the EU Commission.
4. Concerned data subjects include customers, interested parties, subscribers, employees, vendors, consultants, suppliers, commercial agents and contact partners.
5. The draft BCR-C of Elanders Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Elanders Group draft BCR-C contain all elements required under Article 47 GDPR and WP256 rev01, in accordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Elanders Intra-Group Agreement for Compliance with BCR-C, the EDPB considers that the draft decision of the Swedish Supervisory Authority may be adopted as it is, since the draft BCR-C of Elanders Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Swedish Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Swedish Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Swedish Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁶, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental

⁶ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 03/2021 on the draft decision of the Belgian
Supervisory Authority regarding the Controller Binding
Corporate Rules of BDO**

Adopted on 22 January 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of BDO were reviewed by the Belgian Supervisory Authority (Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)) as the Lead SA (hereinafter the "BCR Lead SA")⁶.
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of BDO, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 20 October 2020. The decision on the completeness of the file was taken on 26 November 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁶ Initially, the draft BCR-C of BDO were reviewed by the UK Supervisory Authority (Information Commissioner of the United Kingdom) as the BCRs Lead SA, in accordance with the cooperation procedure as set out in WP263 rev.01.

2 ASSESSMENT

3. The draft BCR-C of BDO cover personal data transferred, directly or indirectly, from BDO members in the EEA to members outside the EEA and processed by those members outside the EEA.
4. Concerned data subjects include clients, employees and business contacts.
5. The draft BCR-C of BDO have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCRs-C of BDO contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake – by signing depending on the respective role and position of each member within the group the ‘Joining Agreement’ or entering into a unilateral declaration – the EDPB considers that the draft decision of the Belgian SA may be adopted as it is, since the draft BCRs -C of BDO contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Belgian Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Belgian Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Belgian Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 04/2021 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of BDO

Adopted on 22 January 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors, (hereinafter "BCR-P"), including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of BDO were reviewed by the Belgian Supervisory Authority (Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA)) as the Lead SA (hereinafter the "BCR Lead SA")⁶.
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-P of BDO, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 20 October 2020. The decision on the completeness of the file was taken on 26 November 2020.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁶ Initially, the draft BCR-P of BDO were reviewed by the UK Supervisory Authority (Information Commissioner of the United Kingdom) as the BCRs Lead SA, in accordance with the cooperation procedure as set out in WP263 rev.01.

2 ASSESSMENT

3. The draft BCR-P of BDO cover personal data transferred, directly or indirectly, from BDO members acting as processors in the EEA to entities of the group outside the EEA and processed by those entities outside the EEA acting as sub-processors.
4. Concerned data subjects include clients for which a BDO member is acting as a processor and suppliers, sub-contractors and other third parties doing business with or interacting with BDO, including client counterparties and advisers.
5. The draft BCR-P of BDO have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of BDO contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake – by signing depending on the respective role and position of each member within the group the ‘Joining Agreement’ or entering into a unilateral declaration – the EDPB considers that the draft decision of the Belgian SA may be adopted as it is, since the draft BCR-P of BDO contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Belgian Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Belgian Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Belgian Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 05/2021 on the draft Administrative Arrangement
for the transfer of personal data between
the Haut Conseil du Commissariat aux Comptes (H3C)
and
the Public Company Accounting Oversight Board (PCAOB)**

Adopted on 2 February 2021

Table of contents

1	Summary of the facts	4
2	Assessment.....	4
3	Conclusions/recommendations	8
4	Final remarks	9

The European Data Protection Board

Having regard to Article 63, Article 64(2), (3) – (8) and Article 46(3)(b) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to EDPB Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies adopted on 15 December 2020,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 10 and Article 22 of its Rules of Procedure,

Whereas:

(1) With reference to Article 46(1), (3)(b) and 46(4) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Subject to authorisation from the competent supervisory authority (“competent SA”), the appropriate safeguards may also be provided for, in particular, by provisions inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(2) Taking into account the specific characteristics of the administrative arrangements provided for by Article 46(3)(b)², which may vary considerably, each case should be addressed individually and is without prejudice to the assessment of any other administrative arrangement.

(3) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

(5) Pursuant to Article 65(1)(c) GDPR where a competent SA does not follow the opinion of the EDPB issued under Article 64, any supervisory authority concerned or the Commission may communicate the matter to the EDPB and it shall adopt a binding decision.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² See also recital 108 GDPR

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Haut Conseil du Commissariat aux Comptes (H3C) has submitted by an official letter addressed to the French Supervisory Authority (Commission Nationale de l’Informatique et des Libertés) a draft Administrative Arrangement (hereinafter draft AA) intended to frame the transfers of personal data from the H3C to the PCAOB in accordance with Article 46(3)(b) GDPR.
2. This draft AA was communicated to the French Supervisory Authority on 19 November 2020.
3. Following the submission, the French Supervisory Authority has requested the Board for an opinion pursuant to Article 64(2) GDPR. The decision on the completeness of the file was taken on 9 December 2020.

2 ASSESSMENT

4. The exchange of personal data between the H3C and the PCAOB is necessary to ensure their audit regulatory functions in accordance with the Sarbanes-Oxley Act and Article 47 of Directive 2006/43/EC of the European Parliament³, namely for the purposes of auditor oversight, inspections and investigations of registered audit firms and their associated persons subject to the regulatory jurisdiction of the PCAOB and the H3C.
5. Other EEA Audit Authorities similarly face a need to exchange personal data with the PCAOB. Thus, the draft AA currently submitted to the EDPB for an opinion might be considered by other EEA Audit Authorities as a model to follow as they seek to frame the same kind of transfers of personal data to the PCAOB in their specific AAs, AA which in turn must be submitted to the competent SA for authorisation. As a result, the subject matter produces effects in more than one Member States within the meaning of Article 64(2) GDPR.
6. In assessing the provisions contained in this specific AA, the EDPB has taken into account a number of specific elements including the type of personal data subject to the AA and the objectives pursued.
7. The draft AA and its Annexes include the following guarantees:

Definitions of concepts and data subject rights:

8. Article I of the AA contains the relevant definitions necessary to determine the scope of the AA and its consistent application. Among them there are some definitions of key concepts and rights of the European data protection legal framework such as “personal data”, “processing of personal data”, “personal data breach”, “right of access” and “right of erasure”.

³ Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC

Principle of purpose limitation and prohibition of any further use:

9. Article III.1 of the AA provides that personal data transferred by the H3C to the PCAOB may be processed by the PCAOB itself only to fulfil its audit regulatory functions in accordance with the Sarbanes - Oxley Act for the purposes of auditor oversight, inspections and investigations of registered audit firms and their associated persons subject to the regulatory jurisdiction of the PCAOB and the H3C. According to the principle of purpose limitation, the transfers can therefore only take place in the framework of such mandates and responsibilities. The PCAOB will not be allowed to process personal data it receives for any purpose other than as set forth in the AA.
10. Indeed, the PCAOB primarily seeks the names, and information relating to the professional activities, of the individual persons who were responsible for or participated in the audit engagements selected for review during an inspection or an investigation, or who play a significant role in the firm's management and quality control. Such information would be used by the PCAOB in order to assess the degree of compliance of the registered accounting firm and its associated persons with the Sarbanes-Oxley Act, the securities laws relating to the preparation and issuances of audit reports, the rules of the PCAOB, the rules of the SEC and relevant professional standards in connection with its performance of audits, issuances of audit reports and related matters involving issuers (as defined in the Sarbanes-Oxley Act).

Principle of data quality and proportionality:

11. According to Article III.2 of the AA the personal data transferred by the H3C must be accurate, adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
12. In addition, each Party will inform the other if it becomes aware that previously transmitted or received information is inaccurate and/or must be updated. Having regard to the purposes for which the personal data have been transferred, the Parties will make any appropriate corrections to their respective files, which may include supplementing, erasing, restricting the processing of, correcting or otherwise rectifying the personal data as appropriate.

Principle of transparency:

13. As provided by Article III.3 of the AA, a general notice to data subjects will be provided by both the H3C and the PCAOB by publishing the AA itself on their websites. In addition to the AA, H3C will provide Information in relation to the processing carried out, including the transfer, the type of entities to which data may be transferred, the rights available to them under the applicable legal requirements, including how to exercise those rights and information about any applicable delay or restrictions on the exercise of such rights and the contact details for submitting a dispute or claim. The PCAOB also will publish on its website appropriate information relating to its processing of Personal Data, including information noted above, as described in the Agreement. Furthermore, individual notice will be provided to data subjects by the H3C in accordance with the GDPR. The H3C will notify the PCAOB in advance of making such individual notification.

Principle of data retention:

14. Article III.2 of the AA provides that personal data must be retained in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed, or for the time as required by applicable laws, rules

and regulations. The Parties shall have in place appropriate record disposal procedures for all information received pursuant to this AA.

Security and confidentiality measures:

15. Article III.4 of the AA envisages that the PCAOB has provided information (Annex I of the AA) describing its technical and organisational security measures to guard against accidental or unlawful destruction, loss, alteration, disclosure of, or access to the personal data. The PCAOB agrees to notify the H3C of any change to the technical and organisational security measures that would adversely affect the protection level afforded for personal data by the AA. The PCAOB will also update the information in Annex I if such changes are made. In the case that the PCAOB provides such notification to the H3C, the H3C would notify the French Data Protection Authority of such changes.
16. The PCAOB has also provided to the H3C a description of its applicable laws and/or rules relating to confidentiality and the consequences for any unlawful disclosure of non-public or confidential information or suspected violations of these laws and/or rules.
17. Finally, in the case where the PCAOB becomes aware of a personal data breach, it will without undue delay and, where feasible, not later than 24 hours after having become aware that it affects such personal data, notify the breach to the H3C. The PCAOB shall also as soon as possible use reasonable and appropriate means to remedy the breach and minimize the potential adverse effects.

Safeguards relating to data subject rights:

18. Article III.5 of the AA provides for safeguards relating to data subject rights. In particular, data subjects whose personal data has been transferred to the PCAOB can exercise his/her data subject rights as defined in Article I(j) of the AA including by requesting that the H3C identifies any personal data that has been transferred to the PCAOB. In addition, data subjects may request directly to the H3C to confirm with the PCAOB that their personal data is complete, accurate and, if applicable, up-to-date and that the processing is in accordance with the principles in this AA. The PCAOB will address in a reasonable and timely manner any such request from the H3C concerning any Personal Data transferred by the H3C to the PCAOB. The data subject can also contact the PCAOB directly.
19. Any restriction to these rights has to be provided by law and should be necessary and will continue only for as long as the reason for the restriction continues to exist. Such restrictions may be allowed to avoid prejudice or harm to supervisory or enforcement functions of the Parties acting in the exercise of the official authority vested in them, such as for the monitoring or assessment of compliance with the Party's applicable laws or prevention or investigation of suspected offenses; for important objectives of general public interest, as recognized in the United States and in France or in the European Union, including in the spirit of reciprocity of international cooperation; or for the supervision of regulated individuals and entities.

Automated decision making:

20. Article III.5 provides that the PCAOB will not take a legal decision concerning a data subject based solely on automated processing of Personal Data, including Profiling, without human involvement.

Special categories of Personal Data/Sensitive Data:

21. Article III.6 provides that special categories of personal data/sensitive data shall not be transferred by the H3C to the PCAOB.

Restrictions on onward transfers:

22. According to Article III.7 of the AA, the PCAOB will only share Personal Data received from the H3C with those entities identified in Annex II of the AA. In the event of such sharing, except for the U.S. Securities and Exchange Commission, the PCAOB will request the prior written consent of the H3C and will only share such personal data if the third party provides appropriate assurances that are consistent with the safeguards in the AA. When requesting such prior written consent, the PCAOB should provide the elements to the H3C, to allow the latter to provide consent, on the type of personal data that it intends to share and the reasons and purposes for which the sharing would take place. If the H3C does not provide its written consent to such sharing within a maximum of ten days, the PCAOB will consult with the H3C and consider any objections it may have. If the PCAOB decides to share the personal data without the H3C written consent, the PCAOB will notify the H3C of its intention to share and the H3C may then decide whether to suspend the transfer of personal data. This decision should be notified to the French Data Protection Authority. Furthermore, as an exception, where the appropriate assurances cannot be provided by the third party, the personal data may be shared with the third party with the consent of the H3C if sharing the personal data is for important reasons of public interest, as recognized in the United States and in France or in the European Union or if the sharing is necessary for the establishment, exercise or defense of legal claims.
23. Regarding the sharing of personal data with the U.S. Securities and Exchange Commission, the PCAOB will obtain from the former appropriate assurances that are consistent with the safeguards in the AA. In addition, the PCAOB will periodically inform the H3C of the nature of personal data shared and the reason it was shared if providing such information will not risk jeopardizing an ongoing investigation. Such restriction regarding information related to an ongoing investigation will continue only for as long as the reason for the restriction continues to exist.
24. Finally, a data subject may request from the H3C certain information related to his or her personal data that has been transferred by the H3C to the PCAOB. It shall be the responsibility of the H3C to provide such information in accordance with applicable legal requirements in the GDPR and the French Data Protection Act.

Redress:

25. Article III.8 of the AA provides for a redress mechanism. There are four layers of redress provided for the data subject in the AA. First, any dispute or claim brought by a data subject concerning the processing of his or her personal data pursuant to the AA may be made to the H3C, the PCAOB, or both, as may be applicable. Each Party will inform the other Party about any such dispute or claim, and will use its best efforts to amicably settle the dispute or claim in a timely fashion.
26. The PCAOB will inform the H3C of reports it receives from data subjects and will consult with the H3C on a response to the matter.
27. Secondly, if a Party or the Parties is/are not able to resolve a concern or complaint made by a data subject and the data subject's concern or complaint is not manifestly unfounded or excessive, the data subject, the Party or Parties may use a first layer of appropriate dispute resolution mechanism conducted by an independent function within the PCAOB, known as the Hearing Officer.
28. Thirdly, the decision reached through this dispute resolution mechanism may be submitted to a second independent review, which would be conducted by a separate independent function known as the Redress Reviewer. The decisions of both the Hearing Officer and the Redress Reviewer are binding on the PCAOB. These dispute resolution mechanisms are described in detail in Annex III of the AA.

29. In situations where the H3C is of the view that the PCAOB has not acted consistent with the safeguards set out in the AA, the H3C may suspend the transfers until the issue is satisfactorily addressed and may inform the Data Subject thereof.
30. Finally, in any case, the data subject may exercise his or her rights for judicial or administrative remedy (including damages) according to French data protection law.

Oversight mechanism:

31. Article III.9 of the AA provides for an oversight mechanism ensuring the implementation of the safeguards of the AA. This oversight mechanism consists of a combination of internal and external oversight.
32. With regards to the internal oversight, each Party will conduct periodic reviews of its own policies and procedures that implement the safeguards of the AA. Upon reasonable request from the other Party, a Party will review its policies and procedures to ascertain and confirm that the safeguards specified in this Agreement are being implemented effectively and send a summary of the review to the other Party.
33. Regarding the external review, upon request by the H3C to conduct an independent review of the compliance with the safeguards in the AA, the PCAOB will notify the Office of Internal Oversight and Performance Assurance (“IOPA”), which is an independent office of the PCAOB, to perform a review to ascertain and confirm that the safeguards in the AA are being effectively implemented. The details of the functioning of IOPA are provided in Annex IV of the AA. IOPA will provide a summary of the results of its review to the H3C once the PCAOB’s governing Board approves the disclosure of the summary to the H3C.
34. Where the H3C has not received the IOPA’s results of its review and is of the view that the PCAOB has not acted consistent with the safeguards specific to its obligations under the AA, the H3C may suspend the transfers to the PCAOB until the issue is satisfactorily addressed by the PCAOB. Such suspension must be notified to the French Data Protection Authority.

3 CONCLUSIONS/RECOMMENDATIONS

35. The EDPB welcomes the efforts made for this AA which includes a number of important data protection safeguards that are in line with the GDPR and also with the safeguards laid down in Guidelines 2/2020 of the EDPB. In order to make sure that these safeguards continue to ensure an appropriate level of data protection when data are transferred to the PCAOB, considering the unique nature of such non-binding agreements, the EDPB underlines the following:

- The French SA will monitor the AA and its practical application especially in relation to Articles III.7, 8 and 9 relating to onward transfers, redress and oversight mechanisms to ensure that data subjects are provided with effective and enforceable data subject rights, appropriate redress and that compliance with the AA is effectively supervised.
- The French SA shall only authorise this AA as a suitable data protection safeguard with a view to the cross-border data transfer, conditional to full compliance by the signatories with all the clauses of the AA.
- The French SA will suspend the relevant data flows carried out by the H3C pursuant to the authorisation, if the AA no longer provides for appropriate safeguards in the meaning of the GDPR.

4 FINAL REMARKS

36. This opinion will be made public pursuant to Article 64(5)(b) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 10/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 23 March 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements	4
2.2	Analysis of the HU SA's accreditation requirements for Code of Conduct's monitoring bodies	5
2.2.1	GENERAL REMARKS	5
2.2.2	INDEPENDENCE	6
2.2.3	CONFLICT OF INTEREST	8
2.2.4	EXPERTISE	9
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	9
2.2.6	TRANSPARENT COMPLAINT HANDLING	10
2.2.7	COMMUNICATION WITH THE HU SA	10
2.2.8	REVIEW MECHANISMS	10
2.2.9	LEGAL STATUS	11
3	CONCLUSIONS / RECOMMENDATIONS	12
4	FINAL REMARKS.....	13

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Hungarian Supervisory Authority (hereinafter "HU SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 26 January 2021.

2 ASSESSMENT

- 2.1 General reasoning of the Board regarding the submitted draft accreditation requirements**
2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the HU SA to take further action.
7. This opinion does not reflect upon items submitted by the HU SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the HU SA’s accreditation requirements for Code of Conduct’s monitoring bodies

8. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board encourages the HU SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements, some examples of the information or documents that applicants have to submit when applying for accreditation.
10. All accreditation requirements submitted to the Board for an opinion must fully address article 41(2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board’s opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1)(p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

11. The Board observes that the draft requirements refer to terms that do not seem equivalent to those included in the Guidelines (section 12, pages 21-25). Examples of such terms include the following: to the authorisation instead of accreditation, associations/organisations owning the code of conduct instead of code owners, criteria instead of requirements, subcontractors instead of external staff, competent supervisory authority instead of NAIH. The Board encourages the HU SA to ensure consistency of the relevant terms throughout the draft accreditation requirements.
12. The Board notes that under section 2 of the draft requirements, there is a reference to the suspension of the accreditation procedure in case of cooperation procedure (GDPR, Article 60 para. 3 and 5) and consistency procedure (GDPR, Article 63 to 66). It is not entirely clear from the draft requirements if this refers to situations where the HU SA investigates a monitoring body that applied for accreditation and there may be a cross-border matter. The Board encourages the HU SA to clarify at this point the connection of the accreditation procedure of a monitoring body with the cooperation and consistency procedures.
13. The Board observes, under section 2, of the HU SA's draft requirements that "*an accreditation term will be initially set at three years at which time there would be a review to ensure that the monitoring body still meets the accreditation criteria*". In addition, the Board notes that the administrative procedure for granting or renewing the accreditation cannot exceed 180 days, as mentioned under section 2 of the requirements. Therefore, the Board understands that a monitoring body that wishes to renew the accreditation, should submit its application at least 180 days before the expiration of the accreditation term. In order to ensure clarity, the Board encourages the HU SA to provide transparent information on what happens after the expiry of the validity of the accreditation and what the procedure will be.
14. Moreover, with regards to the list indicating which monitoring body is responsible for which code members, as mentioned under section 3 of the draft requirements, the Board encourages the HU SA, at the stage of application, to refer to the criteria to distribute their competences instead, since the list of code members may not be fully completed at this stage.
15. The Board observes that section 3 of HU SA's draft accreditation requirements establishes that, when more than one monitoring body is seeking accreditation "the applicant must describe the competence and responsibility of the monitoring body seeking accreditation in the application". The Board welcomes such inclusion but notes that the essential elements of the monitoring body's function should in any case be included in the code itself. To this purpose, the Board recommends that the HU SA clarify in its draft requirements that the core elements of the monitoring body's function will to be included in the code of conduct.

2.2.2 INDEPENDENCE

16. With regard to the accountability of the monitoring body, the Board notes that the monitoring body should be able to demonstrate "accountability" for its decisions and actions in order to be considered independent. The Board considers that the accountability requirements in section 5 of the HU SA's draft accreditation requirements do not fully cover all the elements that should be taken into account. The HU SA should clarify what kind of evidence is expected from the monitoring body, in order to demonstrate accountability. This could be accomplished through such things as setting out roles and decision-making framework and its reporting procedures, and by setting up policies to increase awareness among the staff about the governance structures and the procedures in place. Thus, the Board recommends the HU SA to strengthen the requirements for accountability, to allow for a better

understanding of its content in relation to the independence of the monitoring body, and offer examples of the kind of evidence that the monitoring bodies can provide.

17. With regard to section 5, paragraph 3 of the draft accreditation requirements, the Board takes note of all the elements demonstrating the monitoring body's independence with respect to its organisational structure. Among others, it is stated that the monitoring body must not be penalised for the performance of its tasks. The Board considers that it should be further clarified that the monitoring body assumes responsibility for its activities, and it cannot be penalised by neither the code owner nor the code members. Therefore, the Board encourages the HU SA to redraft this part of the requirements so that the monitoring body is protected against any dismissal or sanction, direct or indirect, for the performance of its duties.
18. With regard to section 5.1 of the draft requirements, the Board observes that the reference to organisational independence of the monitoring body is not entirely complete. The Board notes that monitoring bodies should have the human and technical resources necessary for the effective performance of their tasks. Monitoring bodies should be composed of an adequate number of personnel so that they are able to fully carry out the monitoring functions, reflecting the sector concerned and the risks of the processing activities addressed by the code of conduct. Personnel of the monitoring body shall be responsible and shall retain authority for their decisions regarding the monitoring activities. These organisational aspects could be demonstrated through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel, as well as the duration of the personnel's mandate, contract or other formal agreement with the monitoring body. Therefore, the Board recommends the HU SA to provide suitable requirements for organisational aspects of the independence of the monitoring body and add the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.
19. With regard to section 5.1 and the examples provided to demonstrate the organisational independence of the monitoring body, the Board encourages the HU SA to clarify under the last example provided regarding the documents providing evidence of the business, financial, contractual or other relations between the monitoring body and the association/organisation submitting the code that this applies also code owners and not only to organisations submitting the code.
20. With respect to section 5.1 of the draft requirements, the Board notes that the HU SA refers to the fact that the internal monitoring body reports directly to its highest management level. The Board recommends the HU SA to amend this requirement in order to reflect the requirement, as provided in the Guidelines, that the internal monitoring body has separate management from other areas of the organisation.²
21. Regarding section 5.2 on the financial independence of the monitoring body, the Board notes that the boundary conditions, which determine the concrete requirements for financial independence and sufficient sources, are not been addressed. Such conditions include the size and complexity of the code members (as monitored entities), the nature and scope of their activities (as the subject of the code)

² EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, version 2.0, 4 June 2019, paragraph 65, at https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

and the risk(s) associated with the processing operation(s). Therefore, the Board encourages the HU SA to add the conditions, as above-mentioned to the relevant section of the requirements.

22. Moreover, with regard to section 5.3 “independence of personnel”, the Board observes that the draft accreditation requirements refer to “*appropriate human, technical and logistical resources to effectively perform its monitoring tasks*”. The Board encourages HU SA to redraft the relevant part of the requirements by adding a reference to “sufficient number of sufficiently qualified personnel” and including a reference to technical resources necessary for the effective performance of the monitoring body’s tasks.
23. The Board takes note of the provision under section 5.3 “*resources shall enable the monitoring body to perform its monitoring functions in a fully autonomous, independent and impartial manner*”. However, the Guidelines provide further details on this, stating that the resources should be proportionate to the expected number and size of code members, as well as the complexity or degree or risk of the relevant data processing. Thus, the Board encourages the HU SA to redraft this requirement in line with the Guidelines.
24. In addition, under the same section of the draft accreditation requirements, the Board notes that “*the monitoring body must be responsible for its own personnel within the scope of its tasks and must be entitled to take decisions on its own responsibility and without instructions*”. The Board encourages the HU SA to clarify this paragraph by adding that such instructions should not be taken by the code owners and members within the scope of the code at stake, so to reflect the meaning of the Guidelines.
25. With regard to section 5.4 “independence of decision-making process”, the Board encourages the HU SA to add under this paragraph that the monitoring body shall act independently in its choices and application of sanctions against a controller or processor adhering to the code, so to reflect the meaning of the Guidelines (paragraphs 67, p. 22).

2.2.3 CONFLICT OF INTEREST

26. The Board observes that there is no reference to internal monitoring bodies, which should be appropriately protected from any sort of sanctions or interference by the code owner, other relevant bodies, or members of the code, as a consequence of the fulfilment of its tasks (paragraph 68, page 23 of the Guidelines). The Board encourages the HU SA to provide examples that include internal monitoring bodies.
27. As regard to section 9.1 of the accreditation requirements, the Board encourages the HU SA to clearly state that in order to avoid conflict of interest, the monitoring body must, in particular, be free of external (direct or indirect) influence and, therefore, it shall not seek nor take any instructions from any person or organisation.
28. Moreover, the Board recommends the HU SA to clarify under this section 9.1 that the monitoring body should have its own staff chosen by them or other body independent of the code and that the staff at stake should be subject to the exclusive direction of those bodies only.
29. The Board observes that the requirements under 9.1 of the HU SA accreditation requirements only addresses the situations in which there is a conflict of interest related to the personnel of the monitoring body. The accreditation requirements should also reflect other scenarios where there

might be conflicts of interest of the monitoring body itself, for example, due to its activities, relationships, organisation or procedures. Thus, the Board recommends the HU SA to amend the draft accreditation requirements to reflect that the conflict of interests shall be avoided also in relation to the monitoring body itself, and not only with regard to its staff.

30. Under section 9.1 of HU SA accreditation requirements, there is a reference to the process that the monitoring body shall have in order to avoid and manage conflicts of interest. The Board considers that the measures and procedures in place aiming at preventing conflicts of interest should ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties. Therefore, the Board recommends that the HU SA includes in the accreditation requirements that the procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.
31. The Board encourages the HU SA to add more examples to section 8 on how the monitoring body can demonstrate the mitigation of conflict of interest as well as to include relevant documents to demonstrate how the conflict of interest will be mitigated, such as internal procedure and templates to report a conflict.

2.2.4 EXPERTISE

32. The Board observes that in the accreditation requirements the HU SA makes distinction between legal and technical personnel. The Board encourages the HU SA to clarify that the technical requirements of the personnel will depend on whether this is necessary for the code at stake or not.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

33. The Board observes that the HU SA refers, under section 7, of the requirements to the criteria to be taken into account for the assessment of the established procedures to monitor compliance of the code members with the code and for the periodic review of the operations of the code respectively. However, the Board notes that the complexity and the risks refer to the code concerned and the data processing activities to which the code applies, are not part of such criteria. Therefore, the Board encourages the HU SA to amend this section so to include the complexity and the risks refer to the code at stake and the data processing activities to which the code applies.
34. The Board notes that the HU SA makes reference under section 7.2 to the way that the inspections are conducted. The Board encourages the HU SA to redraft this requirement, to make clear that the inspections will be carried out in an independent manner.
35. In addition to the above, the Board encourages the HU SA to provide equal information in the requirements regarding all the different control methods it deploys (i.e. self-assessment, audits, inspections, questionnaires and regular reporting).
36. The Board observes, that section 7.2, para 5 of the HU SA's draft accreditation requirements, refers to verification requirement without specifying whether it is verification of applications to become code member or verification of compliance of the code members. Therefore the Board encourages the HU SA to redraft the text in order to follow the structure of this section.

2.2.6 TRANSPARENT COMPLAINT HANDLING

37. The Board takes note of the reference under 8.1, third para "*The monitoring body shall demonstrate it has implemented an adequate framework of procedures and structures to receive, investigate and decide on complaints. Such procedures shall be transparent, easily understood and easily accessible to the public as well as adequately resourced so as to ensure effective handling of complaints.*" The Board encourages the HU SA to further clarify this requirement so to make sure that it reflects the obligation to make publicly available decisions or information thereof.

2.2.7 COMMUNICATION WITH THE HU SA

38. Under section 7.5 of the requirements the HU SA refer to the information that will provide to the HU SA. The Board is of the opinion that the requirements need to address such areas as: actions taken in cases of infringement of the code and the reasons for taking them (article 41 (4) GDPR), periodic reports, reviews or audit findings. The code itself will also outline the communication requirements with the CSA, including appropriate ad hoc and regular reports. In the case of serious infringements of the code by code members, which result in serious actions such as suspension or exclusion from the code, the competent SA should be informed without delay. Therefore, the Board encourages the SA to amend this requirement accordingly.
39. The Board observes that the HU SA in its requirements refer to "*changes materially affect the monitoring activities of the monitoring bodies*". The Board is of the opinion that the appropriate word in this context is "substantial change" instead of "material". The Board is of the opinion that "substantial change" covers any change that impacts the monitoring body's ability to perform its function independently and effectively. The Board recommends that the HU SA address the reporting of any substantial change to the HU SA in the accreditation requirements.
40. The Board encourages the HU SA to consider the following practical examples of requirements:
- ✓ A monitoring body shall set out report mechanisms.
 - ✓ A monitoring body shall inform the competent SA, without undue delay, of any substantial change to the monitoring body (particularly related to structure or organisation), which is likely to call into question its independence, expertise and the absence of any conflict of interests or to adversely affect its full operation.
41. The Board notices that sections 7.5 "Providing regular and event-relevant information about monitoring body activity to the supervisory authority" and section 8.3 "Communication with the supervisory authority regarding complaints" overlap. Therefore, the Board encourages that the HU SA merges these two section into one.
- ### **2.2.8 REVIEW MECHANISMS**
42. In the HU SA's draft accreditation requirements, section 7.4 refers to confidentiality. In particular, under this section it is stated that "*the monitoring body is entitled to disclose confidential information to the NAIH in order to help carrying out its supervisory authorities*". This last sentence seems to limit the duty of the monitoring body to cooperate with the HU SA. Therefore, the Board recommends that that this sentence is modified to reflect that the monitoring body is compelled to disclose all information to the HU SA.

43. The Board notices that under section 7.3 of the requirements, the HU SA makes reference to the review of the code. The Board recommends that the HU SA amend this requirement so to include that the new technological developments which may have an impact upon data processing carried out or the provisions of the code should be also taken into account for the review of the code.

The Board notes that under section 7.3 of the requirements there is no reference to the fact that the updating of the code of conduct is the responsibility of the code owner. The Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. Therefore, the Board encourages the HU SA to amend this section accordingly so to include such reference to the code owner.

2.2.9 LEGAL STATUS

44. The Board observes that under section 4 regarding the legal status, the obligation of Article 41(4) of the GDPR together with the section 12.8 of the Guidelines is not reflected in the draft requirements. Therefore, the Board recommends that this section is modified in order to include that the monitoring body and its related governance structures need to be created in a manner that the code owners can demonstrate that the monitoring body has the appropriate standing to carry out its role under Article 41(4) of the GDPR.
45. The Board notes that under section 4 of the draft accreditation requirements, “the monitoring body must be a legal entity with a registered office, or if a natural person, have their headquarters or domicile, to exercise the professional activity as monitoring body in the European Economic Area”. The Board encourages the HU SA to clarify under this section, that not only the natural persons, but also legal entities must have their headquarters in the European Economic Area to exercise a professional activity as monitoring bodies.
46. The Board observes that the HU SA’s draft accreditation requirements mention under section 4 that natural persons can be accredited as a monitoring body. The Board encourages the HU SA to provide additional requirements in order to demonstrate the availability of adequate resources for the specific duties and responsibilities, as well as the full operation of the monitoring mechanism over time. Examples and scenarios to consider include: in the case of resignation or temporary inability of the person concerned.
47. The Board recommends that the HU SA require that the monitoring body should have access to adequate financial and other resource requirements to fulfil its monitoring responsibilities, especially for the accreditation of a natural person.
48. In addition, the Board considers that the existence of sufficient financial and other resources should be accompanied with the necessary procedures to ensure the functioning of the code over time. Thereby, the Board encourages that the HU SA amend the relevant section of the draft accreditation requirements adding the above mentioned reference to “procedures” in addition to the “financial and other resources”.
49. Moreover, the code of conduct itself will need to demonstrate that the operation of the code’s monitoring mechanism is sustainable over time, covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, it would be advisable to require that the monitoring body demonstrates that it can deliver the code of conduct’s monitoring

mechanism over a suitable period of time. Therefore, the Board recommends HU SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.

50. The Board observes that under section 4 "*if the monitoring body is a natural person then it must prove that it has the necessary human resources and, in the event of unforeseen event leading to a sudden, temporary or permanent loss of the monitoring body, the monitoring activities may continue uninterrupted*". The Board encourages the HU SA to clarify that this requirement does not apply only to natural persons, but that it becomes even more essential when the monitoring body is natural person.
51. In addition, for purposes of clear and consistent structure of the draft requirements, the Board encourages the HU SA to move the third paragraph of section 4 "*If the monitoring body is a natural person than it must prove that it has the necessary human resources and, in the event of an unforeseen event leading to a sudden, temporary or permanent loss of the monitoring body, the monitoring activities may continue uninterrupted*" to section 5.3 "independence of personnel" of the draft accreditation requirements.
52. The Board notes that the HU SA's requirements allow for the use of subcontractors. However the Board is of the opinion that the monitoring body should be the ultimate responsible for all decisions taken regarding its monitoring function. Therefore, the Board encourages the HU SA to specify that, notwithstanding the subcontractors' responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance.

3 CONCLUSIONS / RECOMMENDATIONS

53. The draft accreditation requirements of the HU Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
54. Regarding *general remarks* the Board recommends that the HU SA:
 1. amend their draft requirements to make sure that the latter are consistent with the eight areas outlined by the Board in the accreditation section of the Guidelines 1/2019 on codes of conduct and monitoring bodies under the GDPR.
55. Regarding *independence* the Board recommends that the HU SA:
 1. strengthen the requirements for accountability under section 5 of the draft requirements, to allow for a better understanding of its content in relation to independence of the monitoring body, and offer examples of the kind of evidence that the monitoring body can provide.
 2. provide, under section 5.1 of the draft requirements, suitable requirements for organisational aspects of the independence of the monitoring body and add references, as mentioned under para. 18 of this opinion, regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.
 3. amend this requirement so to clarify that the internal monitoring body has separate management of other areas of the organisation.

4. clarify in its draft requirements that the core elements of the monitoring body need to be included in the code itself.
56. Regarding *conflict of interest* the Board recommends that the HU SA:
1. clarify under section 9.1 that the monitoring body should have its own staff chosen by them or other body independent of the code and that the staff at stake should be subject to the exclusive direction of those bodies.
 2. amend its draft accreditation requirements to reflect that the conflict of interests shall be avoided also in relation to the monitoring body itself, and not only with regard to its staff.
 3. include in the accreditation requirements that the procedures and measures in place to avoid conflict of interest ensure that the monitoring body shall refrain from any action incompatible with its tasks and duties.
57. Regarding *communication with the HU SA* the Board recommends that the HU SA:
1. address the reporting of any substantial change to the HU SA in the accreditation requirements.
58. Regarding *review mechanisms* the Board recommends that the HU SA:
1. modify the sentence "*the monitoring body is entitled to disclose confidential information to the NAIH in order to help carrying out its supervisory authorities*" so to reflect that the monitoring body is compelled to disclose all information to the HU SA.
 2. amend the requirement provide under section 7.3 to include that the new technological developments which may have an impact upon data processing carried out or the provisions of the code should be also taken into account for the review of the code.
59. Regarding *legal status* the Board recommends that the HU SA:
1. modify section 4 in order to include that the monitoring body and its related governance structures need to be created in a manner that the code owners can demonstrate that the monitoring body has the appropriate standing to carry out its role under Article 41(4) of the GDPR.
 2. include in the draft requirements the fact that the monitoring body should have access to adequate financial and other resource requirements to fulfil its monitoring body responsibilities, especially for the accreditation of a natural person.
 3. explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time.

4 FINAL REMARKS

60. This opinion is addressed to the Hungarian Supervisory Authority and will be made public pursuant to Article 64 (5) (b) GDPR.
61. According to Article 64 (7) and (8) GDPR, the HU SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to

follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.

62. The HU SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



**Opinion 16/2021 on the draft decision of the Belgian
Supervisory Authority regarding the “EU Data Protection
Code of Conduct for Cloud Service Providers” submitted by
Scope Europe**

Adopted on 19 May 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	4
2.1	The Code of conduct meets the needs of the sector	4
2.1.1	Presentation of the sector	4
2.1.2	The code owner as a representative organisation	5
2.1.3	Processing Scope.....	5
2.1.4	Territorial scope.....	6
2.2	The code of conduct facilitates the effective application of the GDPR	6
2.2.1	The code as a practical tool.....	6
2.2.2	Matrix of requirements.....	6
2.2.3	Binding nature of the Code	7
2.2.4	The Code provides sufficient safeguards and added value	7
2.2.5	The Code as an accountability tool.....	7
2.3	The code of conduct provides effective mechanisms for monitoring compliance with a code 7	
2.3.1	Adherence to the Code	7
2.3.2	The monitoring of the Code	8
2.3.3	Sanctions	8
2.3.4	The review of the code.....	8
3	CONCLUSIONS / RECOMMENDATIONS.....	9
4	FINAL REMARKS.....	9

The European Data Protection Board

Having regard to Article 63, Article 64(1)(b) and Article 40 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) Member States, Supervisory Authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct (hereinafter “code”) to contribute to the proper application of the GDPR².
- (2) The main role of the European Data Protection Board (hereinafter “the EDPB”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve a code of conduct that relates to processing activities in several Member States (hereinafter “transnational code”) pursuant to Article 40.7 GDPR and to the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”).
- (3) The EDPB welcomes and acknowledges the efforts made by the associations and other bodies representing categories of controllers or processors to elaborate codes of conduct which are practical and potentially cost effective tools to ensure greater consistency among a sector and foster the right to privacy and data protection of data subjects by increasing transparency.
- (4) This opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors and to highlight the core elements which each code of conduct has to develop.
- (5) Taking into account the specific characteristics of the sector concerned, each code of conduct should be addressed individually and is without prejudice of the assessment of any other code of conduct. The EDPB recalls that Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost-effective manner that takes on board the specificities for a particular sector and/or its processing activities.
- (6) The EDPB underlines that codes of conduct are voluntary accountability tools, and that the adherence to a code does not prevent SAs from exercising their enforcement power and prerogatives.
- (7) The present code is not a code of conduct according to Article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² Article 40(1) of the GDPR.

terms referred to in point (e) of Article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of chapter V of the GDPR are respected.

- (8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in guidelines on codes of conduct³, the “EU Data Protection Code of Conduct for Cloud Service Providers” (“EU Cloud Code” or “Code”) was reviewed by the Belgian Supervisory Authority as the Competent Supervisory Authority (hereinafter the “CompSA”).
2. The EU Cloud Code has been reviewed according to the procedures set up by the EDPB.
3. The BE SA has submitted its draft decision regarding the EU Cloud Code, requesting an opinion of the EDPB pursuant to Article 64(1)(b) GDPR on 29 February 2021. The decision on the completeness of the file was taken on 31 March 2021.

2 ASSESSMENT

2.1 The Code of conduct meets the needs of the sector

2.1.1 Presentation of the sector

4. Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.
5. The EU Cloud Code aims to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector.
6. The term "cloud computing" covers a variety of very distinct service provision models such as Cloud Infrastructure as a Service Cloud ("IaaS"), Cloud Software as a Service ("SaaS") and Cloud Platform as a Service ("PaaS"). The term "IaaS" describes a situation in which a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. When providing "SaaS", a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. When providing "PaaS", a provider offers solutions for the advanced development and hosting of applications. These services are usually addressed to market

³ Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/676 adopted by the EDPB on 4 June 2019.

players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties.

2.1.2 The code owner as a representative organisation

7. Codes of conduct must be submitted for approval to the supervisory authority which is competent in accordance with Article 55 of the GDPR. In case of transnational codes, when identifying the competent SA, some factors could be taken into account, for example, the location of the largest density of the processing activity or the location of the code owner's headquarters.⁴
8. The EU Cloud Code owner is "Scope Europe" a non-profit association established in Belgium.
9. The code owner has identified the Belgian supervisory authority as the competent supervisory authority for the purposes of seeking approval of the Eu Cloud Code. The code owner has justified its choice in the code of conduct based on the fact that the code owner's and monitoring body's headquarters are based in Belgium.
10. In accordance with Article 40 (2) GDPR, a code of conduct has to be prepared by associations or others bodies representing categories of controllers or processors (code owners). Because the code owner plays a major role in ensuring consistency and harmonization of practices within the sector concerned by the code, it has to demonstrate to the CompSA that it is an effective representative organization. As such, as stated in the Guidelines, the code owner should be capable of understanding the needs of their members and define the processing activity or sector to which the code is intended to apply.⁵
11. Recital 99 GDPR advises to consult during the process of drawing up a Code of Conduct with relevant stakeholders. A group of representatives from European and multinational cloud providers and customers, technical and legal experts, public administrations and others⁶, developed a first foundation of the Code and safeguarded the involvement of different stakeholders and interest groups from early on. The Code was handed over to the EU Cloud Code General Assembly in February 2017.
12. The EU Cloud Code represents several organizations including cloud service providers and associations representing cloud service providers which constitute the General Assembly of the EU Cloud Code.
13. The code owner has demonstrated in the draft code that it is an effective representative body, capable of understanding the needs of their members.

2.1.3 Processing Scope

14. The main objective of the EU Cloud Code is to concretize the legal requirements of Art. 28 GDPR and the relevant related articles of the GDPR. The EU Cloud Code is intended to address all service types of the cloud market (e.g. IaaS, PaaS, SaaS) and creates a "baseline for implementation of GDPR" for these services. Its purpose is to provide practical guidance and define specific requirements for the cloud service providers ("CSPs").
15. The EU Cloud Code only applies to cloud services where the CSP is acting as a processor. It therefore does not apply to "business to consumer" (B2C) services or for any processing activities for which the CSP may act as a data controller. However, the Code is also relevant for consumers who will get

⁴ See Appendix 2 to the Guidelines.

⁵ See para 22 of the Guidelines.

⁶ CSIG – Cloud Select Industry Group - <https://ec.europa.eu/digital-single-market/en/news/cloud-select-industry-group-csig-plenary-meeting>.

additional guarantees of compliance when entrusting with their personal data a company which uses a processor which adheres to the Code.⁷

2.1.4 Territorial scope

16. The scope of the EU Cloud Code is transnational and is intended to apply across the EEA, as per Article 40 (7) GDPR. Scope Europe has identified all European Union and European Economic Area supervisory authorities as concerned SAs.

2.2 The code of conduct facilitates the effective application of the GDPR

17. The EDPB Guidelines precise that Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. A code shall not just re-state the GDPR. Instead, it should aim to codify how compliance with the GDPR can be achieved in a specific, practical and precise manner.⁸ Furthermore, the code has to provide sufficient appropriate safeguards to mitigate the risk around data processing and the right and freedoms of individuals.⁹
18. The EU Cloud Code contains both strict requirements particularizing the provisions of the GDPR mentioned in the “Processing Scope” section of the present Opinion and good practices currently followed by the sector. The Code aims to create comparability between different data processing practices in the cloud industry and improves upon the state of the art for data protection in this sector.

2.2.1 The code as a practical tool

19. The EU Cloud Code aims for all service types of the cloud market (e.g. IaaS, PaaS, SaaS) to concretize the legal requirements of Art. 28 GDPR and the relevant related articles of the GDPR. The Code describes the rights and obligations of adhering CSPs on key principles of GDPR such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.

2.2.2 Matrix of requirements

20. The Code consists of a set of requirements that CSPs have to implement to comply with the Code.
21. Those requirements are supported by a “controls catalogue” helping to assess compliance with the requirements of the Code. The “controls catalogue” maps the requirements of the Code to auditable elements (“controls”), and also maps requirements of the Code to corresponding provisions of the GDPR and relevant international standards, thus facilitating its application and interpretation and enabling implementation, monitoring and where required auditing.
22. The “controls” are to be read in conjunction with the “control guidance” which give advice on how to implement the “controls”.

⁷ It shall be noted, that the adherence of a processor to the Code of Conduct does not entail an automatic recognition of compliance of the processing carried out by such processor nor waives the responsibility of the controller to ensure compliance for all the processing operations carried out on its behalf. In this particular case, the EDPB recalls that the Code of Conduct won't apply to all the processing operations carried out on behalf of the controller, but only to the elements of Article 28 GDPR and related relevant articles. In addition, it shall be recalled that, in this case, the monitoring of the EU Cloud Code of Conduct is based on a service-level approach. Thus, members of the Code are not expected to adhere to the Code with regard to all the elements of all their processing activities, but they can declare which of their services are to be considered compliant with the Code.

⁸ Para 36-37 of the Guidelines.

⁹ Para 39 of the Guidelines.

23. The Code develops requirements which are unambiguous, concrete, attainable and enforceable. All the requirements are consolidated in a control framework, which ensures transparency for all Code's members and data subjects. The EDPB welcomes the use of this kind of tool.

2.2.3 Binding nature of the Code

24. All provisions of the Code and the "controls catalogue" are binding, wherever the provisions make use of "shall", "must". Some provisions should be regarded as guidance, setting examples of good practices and are denoted by the use of the terms "should" or "may".

2.2.4 The Code provides sufficient safeguards and added value

25. In line with the Guidelines¹⁰, a code of conduct must provide sufficient safeguards while being adequately focused on particular data protection areas and issues in the specific sector to which it applies ("added value"). The EU Cloud Code provides sufficient safeguards by, for instance adopting the same terminology as the one used in the GDPR (Code, section 2) and providing complaint mechanism to data subjects (Code, section 7.8.2). In terms of added value, the Code provides guidance adapted to the sector on, among others, security measures, auditing requirements, data subject rights and transparency requirement.

2.2.5 The Code as an accountability tool

26. The objective of the EU Cloud Code is to help CSPs to demonstrate compliance with Article 28 GDPR and make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case in line with Article 28.1 GDPR, which provides that controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject, and Article 28.5 GDPR which states that the adherence of a processor to an approved code of conduct may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of Article 28 GDPR.

2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code

27. As per Article 40(4) of the GDPR and the Guidelines,¹¹ a code requires the implementation of suitable mechanisms to ensure that its rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements

2.3.1 Adherence to the Code

28. The code has to detail an adhesion mechanism.
29. An effective adhesion mechanism has to develop a process divided on three phases which coincide with the code of conduct "lifetime". During the first phase, the mechanism must precise that the code members must comply with all the Code requirements and that the monitoring body will assess the eligibility of candidate to the code. In a second phase, the mechanism shall describe how that monitoring is carried out on an ongoing basis and in a third phase on ad hoc basis.¹² The EU Cloud Code develops an adhesion mechanism which fulfills the three phases of monitoring.

¹⁰ Para 36 of the Guidelines.

¹¹ See para 40 of the Guidelines.

¹² See para 70 of the Guidelines.

2.3.2 The monitoring of the Code

30. The Guidelines indicate that a code will need to identify an appropriate body which has at its disposal mechanisms to enable that body to provide for the effective monitoring of compliance with the code.¹³ As per Article 41 (1) GDPR, The monitoring body identified by the Code has to be accredited by the CompSA¹⁴. Consequently, the CompSA will act as a single point of contact with the code owner and the monitoring body.
31. The EU Cloud Code has appointed “Scope Europe” as monitoring body in accordance with Article 41 of the GDPR. This monitoring body will be in charge of ensuring compliance of the members of the Code with the provisions of the EU Cloud Code and taking actions including sanctions in case of infringement to the provisions of the EU Cloud Code. Decisions taken by the monitoring body relating to its monitoring function (for instance regarding the interpretation of the Code’s rules) shall not be submitted to another entity for approval. Indeed, the monitoring body has to be independent in its mission.
32. The EDPB acknowledges that the EU Cloud Code contains a mechanism which enables the monitoring body to carry out its monitoring functions, as per article 40 (4) of the GDPR.
33. Finally, the EDPB recalls that the code of conduct will not be operational before the designated monitoring body is accredited

2.3.3 Sanctions

34. In accordance with article 40 (4) of the GDPR and the Guidelines, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring body designated by the code owner shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor. Those sanctions range from non-public but formal reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the competent supervisory authority about any related actions taken (Code, section 7.9).
35. To ensure transparency to code members, the code shall include a list of corrective measures which must be applied by the monitoring body. For this purpose, the EU Cloud Code develops an enforcement framework which determines the appropriate sanction to be followed by the monitoring body (Code, section 7.9).

2.3.4 The review of the code

36. As per Article 40 (2) of the GDPR and the Guidelines, the code sets out an appropriate review mechanism to ensure that the code remains relevant to legal and technical standards. In particular, section 8.2 of the EU Cloud Code provides that a regular review of the Code to reflect legal, technological or operational changes and best practices shall take place when appropriate.

¹³ See para 40 of the Guidelines.

¹⁴ In accordance with the consistency mechanism referred to in Article 63 of the GDPR, the EDPB adopted an Opinion 2/2020 on the Belgium data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41GDP on 28 January 2020. The monitoring body designated by the code owner of the EU Cloud Code will have to be accredited by the Belgian SA and therefore will have to demonstrate that it fulfills the requirements imposed by article 41 of the GDPR.

3 CONCLUSIONS / RECOMMENDATIONS

37. By way of conclusion, the EDPB considers that the draft code complies with the GDPR, since the EU Cloud Code fulfills the requirements imposed by Article 40 and 41 GDPR.
38. Finally, the EDPB also recalls the provisions contained within Article 40(5) GDPR, in case of amendment or extension of the EU Cloud Code, the CompSA will have to submit the modified version to the EDPB in accordance with the procedures outlined in the Guidelines approved by the EDPB.

4 FINAL REMARKS

39. This opinion is addressed to the BE SA and will be made public pursuant to Article 64(5)(b) GDPR.
40. According to Article 64(7) and (8) GDPR, BE SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
41. Pursuant to Article 70(1)(y) GDPR, the BE SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
42. As per Article 40 (8) GDPR, the Board shall submit this opinion to the European Commission.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)

Adopted on 19 May 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	4
2.1	The Code of conduct meets the needs of the sector	4
2.1.1	Presentation of the sector	4
2.1.2	The code owner as a representative organisation	5
2.1.3	Processing Scope.....	5
2.1.4	Territorial scope.....	6
2.2	The code of conduct facilitates the effective application of the GDPR	6
2.2.1	The code as a practical tool.....	6
2.2.2	Matrix of requirements.....	6
2.2.3	Binding nature of the Code	6
2.2.4	The Code provides sufficient safeguards	6
2.2.5	The Code as an accountability tool.....	7
2.3	The code of conduct provides effective mechanisms for monitoring compliance with a code 7	
2.3.1	Adherence to the Code	7
2.3.2	The monitoring of the Code	7
2.3.3	Sanctions	8
2.3.4	The review of the code.....	8
3	CONCLUSIONS / RECOMMENDATIONS.....	8
4	FINAL REMARKS.....	8

The European Data Protection Board

Having regard to Article 63, Article 64(1)(b) and Article 40 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) Member States, Supervisory Authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct (hereinafter “code”) to contribute to the proper application of the GDPR².
- (2) The main role of the European Data Protection Board (hereinafter “the EDPB”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve a code of conduct that related to processing activities in several Member States (hereinafter “transnational code”) pursuant to article 40.7 GDPR and to the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”).
- (3) The EDPB welcomes and acknowledges the efforts made by the associations and others bodies representing categories of controllers or processors to elaborate codes of conduct which are practical and potentially cost-effective tools to ensure greater consistency among a sector and foster the right to privacy and data protection of data subjects by increasing transparency.
- (4) This opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors and to highlight the core elements which each code of conduct has to develop.
- (5) Taking into account the specific characteristics of the sector concerned, each code of conduct should be addressed individually and is without prejudice of the assessment of any other code of conduct. The EDPB recalls that Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost-effective manner that takes on board the specificities for a particular sector and/or its processing activities.
- (6) The EDPB underlines that codes of conduct are voluntary accountability tools, and that the adherence to a code does not prevent DPAs from exercising their enforcement power and prerogatives.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² Article 40(1) of the GDPR

- (7) The present code is not a code of conduct according to article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation shall take place only if the provisions of chapter V of the GDPR are respected.
- (8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

- 1. In accordance with the cooperation procedure as set out in the guidelines on codes of conduct³, the code of conduct of CISPE (“CISPE Code” or “Code”) was reviewed by the French Supervisory Authority as the Competent Supervisory Authority (hereinafter the “CompSA”).
- 2. The CISPE Code has been reviewed according to the procedures set up by the EDPB.
- 3. The FR SA has submitted its draft decision regarding the draft CISPE Code, requesting an opinion of the EDPB pursuant to Article 64(1)(b) GDPR on 29 February 2021. The decision on the completeness of the file was taken on 31 March 2021.

2 ASSESSMENT

2.1 The Code of conduct meets the needs of the sector

2.1.1 Presentation of the sector

- 4. Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.
- 5. The CISPE Code aims to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector.
- 6. The term “cloud computing” covers a variety of very distinct service provision models such as Cloud Infrastructure as a Service Cloud (“IaaS”), Cloud Software as a Service (“SaaS”) and Cloud Platform as a Service (“PaaS”). The term “IaaS” describes a situation in which a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company’s premises and/or use the leased infrastructure alongside the corporate systems. When providing “SaaS”, a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. When providing “PaaS”, a provider offers solutions for

³ Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/676 adopted by the EDPB on 4 June 2019.

the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties.

2.1.2 The code owner as a representative organisation

7. Codes of conduct must be submitted for approval to the supervisory authority which is competent in accordance with article 55 of the GDPR. In case of transnational codes, when identifying the competent SA, some factors could be taken into account, for example, the location of the largest density of the processing activity or the location of the code owner's headquarters.⁴
8. The Cloud Infrastructure Service Providers (CISPE) is a non-profit association established in Belgium.
9. The code owner has identified the French supervisory authority as the competent supervisory authority for the purposes of seeking approval of the CISPE Code. The code owner has justified his choice in the code of conduct based on several criteria such as the establishment of several CISPE members in France or the establishment of officers of CISPE including the treasurer and the chairman's companies in France.
10. In accordance with Article 40 (2) GDPR, a code of conduct has to be prepared by associations or others bodies representing categories of controllers or processors (code owners). Because the code owner has a major role in ensuring consistency and harmonization of practices within the sector concerned by the code, it has to demonstrate to the CompSA that it is an effective representative organization. As such, as stated in the Guidelines, the code owner should be capable of understanding the needs of their members and define the processing activity or sector to which the code is intended to apply.⁵
11. Recital 99 GDPR advises to consult during the process of drawing up a Code of Conduct with relevant stakeholders. The CISPE Code has been prepared through a collaborative process between the CISPE members, all of whom are cloud infrastructure service providers (hereinafter "CISPs") providing cloud infrastructure services to European customers. CISPE is intended to represent CISPs and includes representatives from market leading CISPs offering services throughout Europe, across many EU member states. All relevant stakeholders have been consulted and asked to approve the CISPE code of conduct. In this way, the Code provides a summary of stakeholder's consultations.
12. The code owner has demonstrated in the draft Code that it is an effective representative body, capable of understanding the needs of their members.

2.1.3 Processing Scope

13. The CISPE Code applies to the specific features of processing by IaaS providers. It seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. The Code requirements set out the GDPR principles which CISPs, as data processors, must respect. It therefore does not apply to "business to consumer" (B2C) services or for any processing activities for which the CISP may act as a data controller. However, the code is also relevant for consumers who will get additional guarantees of compliance when entrusting with their personal data a company which uses a processor which adheres to the Code.⁶

⁴ See Appendix 2 to the Guidelines.

⁵ See para. 22 Guidelines.

⁶ It shall be noted, that the adherence of a processor to the Code of Conduct does not entail an automatic recognition of compliance of the processing carried out by such processor nor waives the responsibility of the

2.1.4 Territorial scope

14. The scope of the CISPE Code is transnational and is intended to apply across the EEA, as per article 40 (7) GDPR. The CISPE Code has identified all European Union and European Economic Area supervisory authorities as concerned SAs.

2.2 The code of conduct facilitates the effective application of the GDPR

15. The Guidelines precise that Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. A code shall not just re-state the GDPR. Instead, it should aim to codify how compliance to GDPR can be achieved in a specific, practical and precise manner.⁷ Furthermore, the code has to provide sufficient appropriate safeguards to mitigate the risk around data processing and the right and freedoms of individuals.⁸
16. The CISPE Code contains both strict requirements particularizing the provisions of the GDPR mentioned in the “Processing Scope” section of the present Opinion and good practices currently followed by the sector. The CISPE Code helps CISPs to understand clearly what their obligations are under the GDPR, facilitates best practice compliance by IaaS providers and improves upon the state of the art for data protection in the Cloud sector

2.2.1 The code as a practical tool

17. The Code seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. The CISPE Code describes the rights and obligations of adhering CISPs on the basis of key principles of GDPR such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.

2.2.2 Matrix of requirements

18. The Code consists of a set of requirements that CISPs have to implement to comply with the Code.
19. The Codes develops requirements which are unambiguous, concrete, attainable and enforceable. All the requirements are consolidated in a control framework, which ensures transparency for all Code’s members and data subjects and facilitates its application and interpretation, enabling implementation, monitoring and where required auditing. The EDPB welcomes the use of this kind of tool.

2.2.3 Binding nature of the Code

20. All provisions of the Code are binding, wherever the provisions make use of “shall”, “must”. Some provisions should be regarded as guidance, setting examples of good practices and are denoted by the use of the terms “should” or “may”.

2.2.4 The Code provides sufficient safeguards

21. In line with the Guidelines,⁹ a code of conduct must provide sufficient safeguards while being adequately focused on particular data protection areas and issues in the specific sector to which it applies (“added value”). The CISPE Code provides sufficient safeguards by, for instance adopting the

controller to ensure compliance for all the processing operations carried out on its behalf. In this particular case, the EDPB recalls that the Code of Conduct won’t apply to all the processing operations carried out on behalf of the controller, but only to the elements of Article 28 GDPR and related relevant articles. In addition, it shall be recalled that, in this case, the monitoring of the CISPE Code of Conduct is based on a service-level approach. Thus, members of the Code might not adhere to the Code with regard to all the elements of all their processing activities, but they can declare which of their services are to be considered compliant with the Code.

⁷ Para 36-37 of the Guidelines.

⁸ Para 39 of the Guidelines.

⁹ See para 36 of the Guidelines.

same terminology as the one used in the GDPR and providing complaint mechanism to data subjects. In terms of added value, the code provides guidance adapted to the sector on, among others, security measures, auditing requirements, data subject rights and transparency requirement.

2.2.5 The Code as an accountability tool

22. The objective of the CISPE Code is to help C ISPs to demonstrate compliance with article 28 GDPR and make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case in line with article 28.1 GDPR which provides that controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject and article 28.5 GDPR which states that the adherence of a processor to an approved code of conduct may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of article 28 GDPR.

2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code

23. As per Article 40(4) of the GDPR and the Guidelines,¹⁰ a code requires the implementation of suitable mechanisms to ensure that its rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements.

2.3.1 Adherence to the Code

24. The code has to detail an adhesion mechanism.
25. An effective adhesion mechanism has to develop a process divided on three phases which coincide with the code of conduct “lifetime”. During the first phase, the mechanism must precise that the code members must comply with all the Code requirements and that the monitoring body will assess the eligibility of candidate to the code. In a second phase, the mechanism shall describe how that monitoring is carried out on an ongoing basis and in a third phase on ad hoc basis.¹¹ The CISPE Code develops an adhesion mechanism which fulfills the three phases of monitoring.

2.3.2 The monitoring of the Code

26. The Guidelines indicate that a code will also need to identify an appropriate body which has at its disposal mechanisms to enable that body to provide for the effective monitoring of compliance with the code.¹² As per Article 41 (1) GDPR, the monitoring body identified by the Code has to be accredited by the CompSA¹³ Consequently, the CompSA will act as a single point of contact with the code owner and the monitoring body.
27. The CISPE Code has appointed several external monitoring bodies in accordance with article 41 of the GDPR. These monitoring bodies will be in charge of ensuring compliance of the members of the Code with the provisions of the CISPE Code and taking actions including sanctions in case of infringement to

¹⁰ See para 40 of the Guidelines.

¹¹ Para 70 of the Guidelines.

¹² Para 40 of the Guidelines.

¹³ In accordance with the consistency mechanism referred to in Article 63 of the GDPR, the EDPB adopted an Opinion 3/2020 on the France data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR on 28 January 2020. The monitoring bodies designated by the code owner of the CISPE code of conduct will have to be accredited by the French SA and therefore will have to demonstrate that they fulfil the requirements imposed by article 41 of the GDPR.

the provisions of the CISPE Code. Decisions taken by these monitoring bodies relating to their monitoring functions (for instance regarding the interpretation of the Code's rules) shall not be submitted to another entity for approval. Indeed, these monitoring bodies have to be independent in their mission.

28. The EDPB acknowledges that the CISPE Code contains a mechanism which enables the monitoring bodies to carry out their monitoring functions, as per article 40 (4) of the GDPR.
29. Finally, the EDPB recalls that the code of conduct will not be operational before the designated monitoring body is accredited.¹⁴

2.3.3 Sanctions

30. In accordance with article 40 (4) of the GDPR and the Guidelines, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring body designated by the code owner shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor. Those sanctions range from non-public but formal reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the competent supervisory authority about any related actions taken.
31. To ensure transparency to code members, the code shall include a list of corrective measures which must be applied by the monitoring body. For this purpose, the CISPE Code develops an enforcement framework which determines the appropriate sanction to be followed by the monitoring bodies.

2.3.4 The review of the code

32. As per article 40 (2) of the GDPR and the Guidelines, the code sets out an appropriate review mechanism to ensure that the code remains relevant to legal and technical standard. In particular, section 7.3 of the CISPE Code provides that a regular review of the Code to reflect legal, technological or operational changes and best practices shall take place when appropriate.

3 CONCLUSIONS / RECOMMENDATIONS

33. By way of conclusion, the EDPB considers that the draft code complies with the GDPR, since the CISPE code of conduct fulfills the requirements imposed by Article 40 and 41 GDPR.
34. Finally, the EDPB also recalls the provisions contained within Article 40(5) GDPR, in case of amendment or extension of the CISPE code of conduct, the CompSA will have to submit the modified version to the EDPB in accordance with the procedures outlined in the guidelines approved by the EDPB.

4 FINAL REMARKS

35. This opinion is addressed to the FR SA and will be made public pursuant to Article 64(5)(b) GDPR.
36. According to Article 64(7) and (8) GDPR, the FR SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
37. Pursuant to Article 70(1)(y) GDPR, the FR SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

¹⁴ Where several monitoring bodies are designated by the code, the accreditation of one of them is sufficient to provide to the code of conduct a binding nature.

38. As per Article 40 (8) GDPR, the Board shall submit this opinion to the European Commission.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 18/2021 on the draft Standard Contractual Clauses
submitted by the LT SA (Article 28(8) GDPR)**

Adopted on 19 May 2021

TABLE OF CONTENTS

1	Summary of the Facts.....	4
2	Assessment.....	4
2.1	General reasoning of the Board regarding the set of standard contractual clauses.....	4
2.2	Analysis of the draft decision and of the draft standard contractual clauses	5
2.2.1	General remark on the whole SCCs and on the draft decision.....	5
2.2.2	Purpose of the agreement (Chapter I of the SCCs).....	6
2.2.3	Obligation of the parties (Chapter II of the SCCs).....	6
2.2.4	Confidentiality (Chapter III of the SCCs).....	7
2.2.5	Security of processing (Chapter IV of the SCCs).....	7
2.2.6	Engagement of other data processor (Chapter V of the SCCs).....	8
2.2.7	Transfer of data to third countries or international organisations (Chapter VI of the SCCs)	9
2.2.8	Assistance to the data controller (Chapter VII of the SCCs)	9
2.2.9	Notification of personal data breach (Chapter VIII of the SCCs).....	10
2.2.10	Erasure and return of data (Chapter IX of the SCCs)	11
2.2.11	Control of the data processor / Audit and inspection (Chapter X of the SCCs)	11
2.2.12	Final provisions (Chapter XI of the SCCs)	11
2.2.13	Annex 1	11
2.2.14	Annex 2	12
2.2.15	Annex 3	12
3	Conclusions	13
4	Final Remarks	13

The European Data Protection Board

Having regard to Article 28(8), Article 63 and Article 64(1)(d), (3) - (8) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter, "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter, the "Board") is to ensure the consistent application of the GDPR throughout the Union. To this end, the Board shall issue an opinion based on Article 64(1)(d) GDPR where a supervisory authority (hereinafter, "SA") aims to determine standard contractual clauses (hereinafter, also "SCCs") referred to in Article 28(8) GDPR. The aim of this Opinion is therefore to contribute to a harmonised approach concerning measures to be adopted by a supervisory authority that are intended to produce legal effects as regards processing operations which substantially affect a significant number of data subjects in several Member States and the consistent implementation of the GDPR's specific provisions.
- (2) In the context of the relationship between a data controller and a data processor (or data processors) for the processing of personal data, the GDPR establishes, in its Article 28, a set of provisions with respect to the setting up of a specific contract between the parties involved and to mandatory provisions that should be incorporated in it.
- (3) According to Article 28(3) GDPR, the processing by a data processor "*shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller*"; a set of specific aspects to regulate the contractual relationship between the parties is therefore set out, including among others, the subject-matter and duration of the processing, its nature and purpose, the type of personal data and categories of data subjects.
- (4) Under Article 28(6) GDPR, without prejudice to an individual contract between the data controller and the data processor, the contract or the other legal act referred in paragraphs (3) and (4) of Article 28 GDPR may be based, in whole or in part, on standard contractual clauses. These standard contractual clauses are to be adopted for the matters referred to in paragraphs (3) and (4).
- (5) Furthermore, Article 28(8) GDPR determines that a SA may adopt a set of standard contractual clauses in accordance with the consistency mechanism referred to in Article 63. In this regard, SAs are required to cooperate with other members of the Board and, where relevant, with the European Commission through the consistency mechanism. Pursuant to Article 64(1)(d), SAs are required to

¹ References to the "Union" or the "EU" made throughout this Opinion should be understood as references to the "EEA".

communicate to the Board any draft decision aiming to determine standard contractual clauses pursuant to Article 28(8). In this context, the Board is required to issue an opinion on the matter, pursuant to Article 64(3), where it has not already issued an opinion on the same matter.

(6) Adopted standard contractual clauses constitute a set of guarantees to be used as is, as they are intended to protect data subjects and mitigate specific risks associated with the fundamental principles of data protection.

(7) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete (unless the period is extended upon decision of the Chair by a further six weeks).

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Lithuanian supervisory authority (hereinafter, "LT SA") has submitted its draft decision and its draft standard contractual clauses to the Board, requesting its opinion pursuant to Article 64(1)(d), for a consistent approach at Union level. After the decision on the completeness of the file, the EDPB Secretariat circulated the file to all members on behalf of the Chair on 26 March 2021.
2. The Board has received the draft SCCs from the LT SA along with a draft decision explaining the background and role of the standard contractual clauses. These two documents were provided by the LT SA in an English version.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the set of standard contractual clauses

3. Any set of standard contractual clauses submitted to the Board under Article 28(8) and Article 64(1)(d) must further specify the provisions foreseen in Article 28 GDPR. The opinion of the Board aims at ensuring consistency and a correct application of Article 28 GDPR as regards the presented draft clauses, which could serve as Art. 28(8) standard contractual clauses.
4. The Board notes that the draft SCCs presented to the Board are composed of two parts:
 - 1) a general part containing general provisions to be used "as is"; and
 - 2) a specific part that has to be completed by the parties with regard to the specific processing which the contract seeks to govern.
5. The Board recalls that the evaluation of each draft decision subject to the consistency mechanism is made individually and on its own merits, bearing in mind the goal of ensuring consistency.

6. The EDPB has already expressed its views on draft standard contractual clauses for the purposes of compliance with Article 28 GDPR in EDPB Opinion 14/2019², EDPB Opinion 17/2020³, and EDPB-EDPS Joint Opinion 1/2021⁴.
7. When this opinion remains silent on one or more clauses of the SCCs submitted by the LT SA, it means that the Board is not asking the LT SA to take further action with regard to those specific clauses.

2.2 Analysis of the draft decision and of the draft standard contractual clauses

2.2.1 General remark on the whole SCCs and on the draft decision

8. Since a contract under Article 28 GDPR should further stipulate and clarify how the obligations in Article 28(3)-(4) will be fulfilled, the SCCs need to be analysed in their entirety.
9. In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority does not prevent the parties from adding other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, the adopted standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Furthermore, where the standard data protection clauses are modified, the parties will no longer be deemed to have implemented adopted standard contractual clauses. Consequently, the Board recommends that the LT SA replace the words "*if they directly or indirectly contradict*" in the draft decision (paragraph 2) by "*as long as they do not directly or indirectly contradict*".
10. The Board notes that the wording of several clauses of the SCCs in the English version provided are not in line with the terminology of the relevant provisions of the GDPR. Examples include: "*controller's duties*" (used instead of "*controller's obligations*"), "*Union or Member State legal acts*" (used instead of "*Union or Member State law*"), "*permission*" (used instead of "*authorization*"), "*prove*" (used instead of "*demonstrate*"), "*special*" (used instead of "*specific*"). The Board therefore recommends the LT SA to align the wording of those clauses with the relevant provisions of the GDPR.
11. Further, the Board is of the opinion that the use of the word "Agreement" to designate SCCs may trigger confusion between this contractual document which serve as Article 28(8) GDPR standard contractual clauses and other possible agreements that might be concluded by the Parties. For the sake of clarity, the Board recommends that the LT SA replace the words "Agreement" by "Standard

² EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), adopted on 9 July 2019, available here:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_en.pdf; The final version of the standard contractual clauses for the purposes of compliance with Article 28 GDPR adopted by the Danish SA is available here: https://edpb.europa.eu/our-work-tools/our-documents/decisionsa/dk-sa-standard-contractual-clauses-purposes-compliance-art_en.

³ EDPB Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 28(8) GDPR), adopted on 19 May 2020, available here:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28scs_si_en.pdf.

⁴ EDPB-EDPS Joint Opinion 1/2021 on the draft Standard Contractual Clauses submitted by the European Commission (Article 28(7) GDPR), adopted on 19 May 2020, available here:

https://edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-12021-standard_en.

Contractual Clauses” or “Clauses” where referring to the aforementioned SCCs, in the whole draft decision and in the whole annex.

12. The Board recommends removing the reference to “*other mutual agreements*” from page 1 (last paragraph) of the draft SCCs as it seems to imply that additional clauses or agreements entered into by the parties fall within the scope of the SCCs themselves.
13. Finally, the Board is of the opinion that a specific provision on the definition of the terms used in the Clauses might be added to the SCCs in order to avoid any difficulties in practice. The Board therefore encourages the LT SA to specify that whenever the Clauses use the terms defined in the GDPR, those terms have the meaning given to such terms by the GDPR itself.

2.2.2 Purpose of the agreement (Chapter I of the SCCs)

14. Regarding **clause 2** of the SCCs, the Board is of the opinion that the wording “[*where applicable, details of the agreement on provision of such services*]” is not fully clear, and encourages the LT SA to further clarify which type of details the parties would be expected to insert. As an example, the clause may be redrafted as follows: “[*where applicable, specify details on the agreement entered into by the Parties on these services, e.g. date / title*]”. In addition, and in order to avoid any doubt regarding what should be filled in by the Parties in Annex 1, the Board encourages the LT SA to replace the words “[*including but not limited to the subject, purpose and nature of the processing of personal data, types of personal data, categories of the data subjects etc.*” with a direct reference to Annex 1.

2.2.3 Obligation of the parties (Chapter II of the SCCs)

15. Regarding **clause 3** of the SCCs, the Board is of the opinion that the reference to commitments that the controller “shall undertake” may be misleading in the context of a contract because the rights and obligations of the controller described in clause 3 are already vested in the controller by the GDPR, and that it should be deleted. In addition, this clause would be clearer if a reference to Article 24 GDPR and its accountability principle were made. Consequently, the Board recommends that clause 3.1 be modified, for instance, as follows: “[*The Data Controller*] is responsible for ensuring that the processing of personal data takes place in compliance with Regulation (EU) 2016/679 (see Article 24 GDPR) [...].”
16. Regarding **clause 3.2** of the SCCs, since the controller has already defined the purposes and means of the processing activity subject to the SCCs, the Board recommends to the LT SA to rephrase it as follows: “[*3.2 [The Data Controller] has the right and obligation to make decisions about the purposes and means of the processing of personal data*].”
17. Regarding **clause 3.3** of the SCCs, the Board is of the opinion that it should be clarified that the obligation of the controller is not limited to the identification of the legal basis, and thus recommends that the clause be redrafted as follows: “[*3.3 [The Data Controller] shall be responsible, among others, for ensuring that the processing of personal data which the data processor is instructed to perform has a legal basis.*”]
18. Regarding **clause 4.1** of the SCCs, third sentence, the Board is of the opinion that the possibility for the controller to give subsequent or further instructions is necessary to fully implement the rights and obligations of the parties set out in the clause 4, but is not unlimited. Any subsequent instruction should be in line with the respective rights and obligations of the parties set out in the SCCs. For the sake of clarity, the EDPB therefore encourages the LT SA to specify this in the clause.

19. Furthermore, the Board considers that where the processor processes the data not under the instructions of the controller but because it is required to do so by Union or Member State law to which it is subject, then the processor shall inform the controller of the legal requirement before the processing of this data, unless that law prohibits such information on important grounds of public interest. The Board therefore recommends to the LT SA to include this specification.

2.2.4 Confidentiality (Chapter III of the SCCs)

20. Regarding **clause 7** of the SCCs, first sentence, the Board recommends, for the sake of consistency and clarity, that the LT SA bring the wording in line with Article 28(3)(b) GDPR and refer explicitly to the principle of the access to the personal data on a “need-to-know” basis. The Board would therefore suggest the following wording: *“under the processor’s authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis”*. Furthermore, the Board encourages the LT SA to split the following part of clause 7 into different paragraphs and introduce some amendments in order to enhance its clarity: clause 7 can therefore be reorganised as follows: *“7. [...] The Parties ensure that: 7.1. In case of a need to change in the persons having access to personal data, their right of access to the Data Controller’s personal data shall be revoked not later than on the last day on which their tasks require them to have access to the personal data of the Data Controller entrusted to the Processor. In case of discontinuation of employment relationship with the employee of the Data Processor, the access rights to the Data Controller’s personal data shall be revoked not later than on the last day of work. 7.2 The list of persons granted access to personal data shall be reviewed on a periodical basis [...]”*.

2.2.5 Security of processing (Chapter IV of the SCCs)

21. Regarding **clause 9** of the SCCs, the Board recommends that the LT SA specify that the level of the risk should take into account *“the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons”*, which corresponds to the wording of Article 32(1) GDPR. This specific wording is used in the GDPR to make sure that the level of security applied to the processing of personal data is always in line with the latest technological evolutions.
22. Regarding **clause 11** of the SCCs, the Board encourages the LT SA to delete *“which may arise”* and to replace *“minimise the risk”* by *“mitigate the risk”*. In addition, the Board recommends to the LT SA to clarify that *“independently from the controller”* refers to the assessment of the risk, rather than to the implementation of measures, which in the current wording is not entirely clear. As an example, the first sentence of the clause may be redrafted as follows: *“According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing activity entrusted to it by the controller, and implement measures to mitigate those risks”*.
23. Regarding **clause 12** of the SCCs, the Board recommends that the LT SA align the wording with Article 28(3)(f) GDPR, by referring to assistance to the controller in ensuring compliance with the obligation (instead of *“fulfilment”* of its *“duties”*) provided for in Article 32 GDPR.
24. Regarding **clause 13** of the SCCs, the Board understands that the first sentence refers to the case where subsequently, in the assessment of the controller, the mitigation of the identified risks requires further measures to be implemented by the processor. If it is the case, the Board recommends to the LT SA to clarify this. As regards the second sentence of the clause, the Board is of the opinion that it

may be misleading to specify the right of the controller to obtain evidence of implementation of such supplementary measures, considering that the audit right of the controller applies more broadly to all the obligations laid down in these SCCs as provided for in Article 28(3)(h) GDPR. The Board therefore recommends to the LT SA to amend this sentence and make reference to Chapter X of the SCCs (e.g. “*The Data Processor shall make available to the Data Controller all information necessary to demonstrate compliance with its obligations as provided in Chapter X of the Clauses*”).

2.2.6 Engagement of other data processor (Chapter V of the SCCs)

25. Regarding Chapter V of the SCCs, the Board encourages the LT SA to slightly rephrase several sentences in order to clarify them. In clause 16, “*for the performance of this Agreement*” could be redrafted as “*for the performance of the processing carried out under this Agreement*”. In clause 16.1, the words “*to the date of engagement*” can be replaced by “*before the date of engagement*”. In clause 16.2, “*no later than till [specify the period]*” can be replaced by “*no later than [specify the period] in advance*” and “*special additional*” by “*specific*”. Finally, the Board suggests avoiding repetition of the reference to Annex 2 in the latest sentences of clauses 16.1 and 16.2 which is already stated in clause 15.
26. Regarding **clause 17** of the SCCs more specifically, the reference to the possibility to enter into a contract or another legal act as currently included in the draft SCCs seems to be potentially misleading. Therefore, the Board recommends that this clause should be aligned with the wording of Article 28(4). In addition, the Board considers that it should be specified in this clause that prior to the processing, the data processor shall inform the sub-processor of the identity and contact details of the controller for which the sub-processor processes personal data. The Board encourages the LT SA to rephrase the clause accordingly, for example as follows: “*Where the Processor engages a sub-processor for carrying out the particular processing on behalf of the Controller, the same data protection obligations as set out between the controller and the processor shall be imposed on the sub-processor by way of a contract or another legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organizational measures so that processing meets the requirements of Regulation (EU) 2016/679. Prior to processing, the data processor shall inform the sub-processor of the identity and contact details of the controller for which the sub-processor processes personal data*”.
27. Regarding **clause 18** of the SCCs, the Board notes that the suggested obligation for the processor to provide a copy of the contract with the sub-processor where there is an impact on the instructions or the level of security is not explicitly provided by the GDPR and may be of unclear application for the parties, but understands the intention of requiring the processor to notify the controller in case of issues arising in connection with the engaged sub-processor. The Board recommends therefore that the LT SA replace this provision with the obligation for the processor to notify to the controller any failure by the sub-processor to fulfil its obligations under the contract or other legal act binding on this sub-processor. Finally, the last sentence should be rephrased as follows: “*The Data Processor is not obliged to provide the provisions of the Agreement on the business-related issues which do not have an impact on the terms and conditions of the legal protection of personal data of the contract concluded with the sub-processor*”.
28. Regarding **clause 19** of the SCCs, the Board understands that the intention is to create a “third party beneficiary right” for the controller within the contract between the data processor and the sub-processor. Therefore, the Board encourages the LT SA to clarify the nature of the clause for instance by redrafting the first sentence as follows: the processor “*shall agree on a third-party beneficiary*

clause with a sub-processor (if any) providing that [...]". The Board also recommends that “*continue data processing relationship directly with the sub-processor*” should be replaced with “*enforce the agreement directly against the sub-processor*”. Additionally, the Board recalls that it sees an added value in having such a clause as part of a standard contractual clauses as it preserves the rights of the controller and therefore recommends to the LT SA to transform it into a non-optional clause.

29. Regarding **clause 20** of the SCCs, the Boards encourages the LT SA to include a reminder that the “*The data processor shall be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR*”.

2.2.7 Transfer of data to third countries or international organisations (Chapter VI of the SCCs)

30. The Board encourages to the LT SA to clarify that the words “third countries” refer to countries outside of the EEA and not outside of Lithuania. This could be carried out by adding in **clause 21** “[...] *third countries (i.e. countries outside of the European Economic Area) [...]"*.
31. In addition, the Board recommends the deletion of footnote 2 in clause 21 and of the same sentence in Annex 3, Point 6 due to the fact that such standard contractual clauses do not appear as the relevant document to elaborate on the definition of the notion of transfers of personal data.
32. Regarding **clause 22** of the SCCs, the Board recommends to replace the wording “*transfer of such information*” with “communication of such information”, in order to avoid any confusion with the notion of transfer as referred to in Chapter V of the GDPR.
33. Regarding **clause 23.1** of the SCCs, the Board encourages the LT SA to clarify the wording as follows: “*to transfer personal data to a Data Controller or a Data Processor in a third country or in an international organisation*”.
34. The Board considers that mentioning the chosen tool for transfers, in addition to the instructions, contributes to demonstrating compliance of the parties with Chapter V of the GDPR; therefore, the EDPB encourages the LT SA to further clarify **clause 24** of the SCCs as follows: “*The data controller's instructions or approval regarding transfers of personal data to a third country including, if applicable, the transfer tool under Chapter V of Regulation (EU) 2016/679 on which they are based, shall be set out in Annex 3 of these standard contractual clauses*”.

2.2.8 Assistance to the data controller (Chapter VII of the SCCs)

35. The Board encourages, for the sake of clarity as well as consistency with Article 28(3)(e) GDPR, the LT SA to slightly rephrase the **clause 26** of the SCCs as follows: “*Taking into account the nature of processing, the Data Processor shall assist the Data Controller to fulfil the Data Controller's obligation to respond to the requests for exercise of the data subject's rights provided for in Chapter III of Regulation (EU) 2016/679 by appropriate technical and organisational measures insofar as this is possible. This implies that the Data Processor shall, insofar as this is possible, assist the Data Controller in its obligation to give effect to the following data subject rights*”.
36. Regarding **clause 27** of the SCCs, the Board notes that the content of this clause is repeated in **clause 29**. The Board therefore encourages the LT SA to merge clause 27 into clause 29, so that the new clause is aimed to ensure that the parties detail the arrangements on the manner the processor is bound to assist the controller relating to data subject rights and data breaches in Annex 3. By way of

example, the new clause could read as follows: “*The Parties shall establish in Annex 3 hereto the appropriate technical and organisational measures which should be taken by the Data Processor to assist the Data Controller with data subject rights and with the obligations under Articles 33 to 36 GDPR, as set out in paragraphs 26 and 27 hereof*”.

37. The Board understands that **clause 28** of the SCCs, coupled with clause 12, is aimed to reflect the content of Article 28(3)(f) GDPR: while clause 12 refers to the processor’s assistance with compliance with Article 32 GDPR, clause 28 covers the processor’s assistance with compliance with Articles 33 to 36 GDPR. As a consequence, the Board recommends that clause 28 refer to clause 12 (rather than 13), and to redraft the clause to ensure closer consistency with the relevant provisions of the GDPR. The clause could be redrafted, for instance, as follows:

“In addition to the Data Processor’s duty to assist the Data Controller in accordance with paragraph 12 hereof, the Data Processor, taking into account the nature of processing and information available to the Data Processor, shall also assist the Data Controller in ensuring compliance with:

- 28.1 the Data Controller’s obligation to, without undue delay and where feasible, [...];*
28.2 the Data Controller’s obligation to notify without undue delay [...]
28.3 the Data Controller’s obligation to carry out a data protection impact assessment [...] where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.
28.4 the Data Controller’s obligation to consult the competent supervisory authority [...] if the data protection impact assessment indicates that processing of data would result in high risk if the Data Controller fails to take measures to mitigate the risk”.

2.2.9 Notification of personal data breach (Chapter VIII of the SCCs)

38. **Clause 30** of the SCCs, second sentence, recommends to the Parties to select a number of hours by which the processor shall notify a data breach which does not exceed 24 hours from the moment of becoming aware of the personal data breach. Such delay may be short in some situations and may also trigger confusion with the delay by which the controller has to notify the personal data breach to the SA. While taking into account the requirement for the processor to notify the controller “*without undue delay*” after becoming aware of the personal data breach in accordance with Article 33.2 GDPR, the Board recommends the LT SA to delete the sentence recommending that the timeframe (which anyways starts from the moment of becoming aware of the personal data breach - the word “breach” is missing) should not exceed 24 hours and allow the parties to choose the appropriate timeframe. Additionally, the Board recommends the deletion of “*If possible*” from the second sentence of clause 30 taking into account that a processor has in any event an obligation to proceed to such notification (Article 33.2 GDPR) and to avoid giving rise to situations where the processor may argue it was “impossible” to notify the controller concerning the data breach within the agreed timeframe.
39. Regarding **clause 31.4** of the SCCs, the Board encourages the LT SA to refer to the “*request of the competent supervisory authority*” instead of the “*letters of the competent supervisory authority*”, since a supervisory authority might request information by means other than letters.
40. Regarding **clause 32** of the SCCs, pertaining to the obligation of the processor to notify additional information in case it fails to provide all information on the occasion of the first notification, the Board recommends that the LT SA remove the reference to 24 hours. Instead, it should be made clear that this information must be provided “*without undue further delay*” (instead of “*immediately*”) in accordance with the controller’s obligation under Article 33(4) GDPR.

2.2.10 Erasure and return of data (Chapter IX of the SCCs)

41. Regarding **clause 34** of the SCCs, the Board recommends that the LT SA specify that the options provided by this clause are left “*at the choice of the controller*” in order to more closely match the wording of Article 28(3)(g) GDPR. In addition, the Board suggests replacing “confirm” by “demonstrate”. Thirdly, the Board recommends clarifying that the deletion of existing copies must be carried out “in any event” (the sentence could be thus rephrased as “[...] *and in any event delete the existing copies unless [...]*”). Finally, the Board recommends that the LT SA detail in the clause itself that the controller should be able to modify the choice made at the time of signature of the contract throughout the life cycle of the contract and upon its termination.

2.2.11 Control of the data processor / Audit and inspection (Chapter X of the SCCs)

42. The Board understands that the Chapter X is referring to Article 28(3)(h) GDPR. The Board therefore encourages the LT SA, for purposes of clarification about the content of this Chapter, to rephrase the **title** of Chapter X as follows: “Audit and inspection of the data processor”.
43. Regarding **clause 37** of the SCCs, the Board encourages the LT SA, for the sake of consistency with the GDPR, to slightly rephrase this clause to align it with the terminology of Article 28(3)(h) GDPR: “*The Data Processor shall make available the Data Controller with all information necessary to demonstrate compliance with the obligation set out in Article 28 of Regulation (EU) 2016/679 and the Agreement and enable and assist the Data Controller or another auditor mandated by the Data Controller to carry out an audit including on-the-spot inspections*”.
44. Regarding **clause 39** of the SCCs, the Board is of the opinion that the wording “physical means” might be misleading. The Board therefore encourages the LT SA to rather refer to “physical facilities”. Further, it may be advisable to specify within the SCCs that the controller and processor commit to cooperating with the Supervisory Authority, including by making available to the authority upon request information aimed to demonstrate compliance, including the results of audits and inspections.

2.2.12 Final provisions (Chapter XI of the SCCs)

45. Regarding **clause 44** of the SCCs, the Board encourages the LT SA to clarify the terms “*materially or regularly breaches the Agreement*” in order to avoid any confusion as to their interpretation by the Parties. In addition to the termination provisions of clause 44, the Board recommends that the SCCs include the possibility for the controller to terminate the SCCs where the clauses have been suspended in accordance with clause 43 of the SCCs and where compliance has not been restored within a certain amount of time to be determined by the Parties.

2.2.13 Annex 1

46. While noting that Annex 1 aims at providing details about the processing activities undertaken by the processor on behalf of the controller, the Board recalls that the processing activities should be described by the parties in the most detailed manner possible. Consequently, the Board welcomes the examples provided by the LT SA to illustrate the possible content of the sections of the Appendix as they are able to guide the parties’ description.
47. The Board is nonetheless of the opinion that slight clarifications can be made on the level of detail expected in the Annex 1. The Board therefore encourages the LT SA to refer to “*processing activities*”

instead of “*processing operations*” in point 1 of the Annex 1, as well was to “*types of personal data*” instead of “*personal data*” in point 1.3 of the Annex 1.

2.2.14 Annex 2

48. Regarding **point 1** of Annex 2, the Board welcomes the inclusion of a table guiding the Parties in the description of authorised sub-processors as provided for in Chapter V of the SCCs.
49. With regard to **point 2** of Annex 2 on prior notification for granting permission to new sub-processors, the Board encourages the LT SA to clarify that this point refers to new sub-processors, not already listed in the previous point. Also, the Board is of the opinion that the first sentence in its current form may be interpreted as contradicting clauses 16.1 and 16.2 which require that a specific period is set, and recommends that the LT SA rephrase the first sentence in order to guarantee that both the period of prior notification and the related terms and conditions are provided by the Parties: “*Please specify the periods of a prior notification of granting permission to the sub-processors and other related terms and conditions*”.

2.2.15 Annex 3

50. Regarding Annex 3 of the SCCs, the Board is of the opinion that several sentences might be rephrased in order to avoid any confusion as to what it is expected to be filled in by the Parties. The Board therefore encourages the LT SA to refer to “*the processing entrusted*” instead of “*the processing assigned*” (point 1), to “*elements*” instead of “*lots*” (point 2), to “*communication of the data*” instead of “*transfer of the data*” (point 2), to “*demonstrate the fact of erasure*” instead of “*prove the fact of erasure*” (point 4), to “*data processing location*” instead of “*data processing place*” (point 5) to “*information*” instead of “*familiarisation*” (points 7 and 8), and to “*physical facilities*” instead of “*physical measures*” (points 7 and 8).
51. As a general remark with respect to **point 2** of Annex 3, relating to Security of Processing, the Board recalls that the degree of detail of the information provided therein must be such as to enable the controller to assess the appropriateness of the measures, in order to comply with its obligation of accountability. Also, a suggestion for the parties to include a description of the measures for the protection of software applications used to process personal data could be useful.
52. Regarding **point 3** of Annex 3 related to the Assistance to Data Controller, the Board is of the opinion that the annex should include the steps to be taken by the processor and the procedure to be followed in providing assistance to the controller with regard to both Article 28(3)(e) and 28(3)(f) GDPR. For example, with regard to the obligation of assistance under Article 28(3)(e) GDPR, it has to be clear in the SCCs whether the data processor is expected to have any contact with the data subjects, and how the processor needs to inform the controller when it comes to data subjects’ rights (e.g. forwarding the request to the controller within a specified timeframe or other appropriate measures). In this case, the assistance is provided only through an exchange of information between the controller and the processor. Another scenario could be that the controller instructs the processor to answer to data subject’s requests according to instructions given. Another option could be that the processor would make the technical implementations instructed by the controller with respect to data subject rights. The Board suggests that the LT SA gives examples of organisational measures under which the cooperation of the processor might be provided in order to indicate the level of detail expected to be filled in by the Parties in Annex 3.

53. The Board also notes that **points 7 and 8** of the Annex 3 state that where the controller carry out a physical examination/on-spot inspection of the processor and sub-processor, it shall bear the costs. As to the issue of allocation of costs between a controller and a processor is not regulated by the GDPR, the Board consequently encourages the LT SA to remove any reference to the costs from these clauses.

3 CONCLUSIONS

54. The Board very much welcomes the Lithuanian SA's initiative to submit its draft SCCs for an opinion which aims at contributing to a harmonised implementation of the GDPR.
55. The Board is of the opinion that the draft SCCs of the Lithuanian Supervisory Authority submitted for an opinion need some further adjustments in order to be considered as standard contractual clauses. If all recommendations listed in this Opinion are implemented, the LT SA will be able to use this draft agreement as Standard Contractual Clauses pursuant to Article 28(8) GDPR without any need for a subsequent adoption from the EU Commission.

4 FINAL REMARKS

56. This opinion is addressed to the Lithuanian *Valstybinė duomenų apsaugos inspekcija* (the Lithuanian Supervisory Authority) and will be made public pursuant to Article 64 (5)(b) GDPR.
57. According to Article 64 (7) and (8) GDPR, the supervisory authority shall communicate to the Chair by electronic means, within two weeks after receiving the opinion, whether it will amend or maintain its draft SCCs. Within the same period, it shall provide the amended draft SCCs or, alternatively, the relevant grounds for which it does not intend to follow this opinion, in whole or in part. The supervisory authority shall communicate the final decision to the Board for inclusion in the register of decisions which have been subject to the consistency mechanism, in accordance with Article 70(1)(y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Adopted

Opinion of the Board (Art. 64)



Opinion 26/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Controller Binding Corporate Rules of the Internet Initiative Japan Group

Adopted on 2 August 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.
- (2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (“BCR Lead”) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.
- (3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers the EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the Internet Initiative Japan Group ("IIJ") were reviewed by the Supervisory Authority of North Rhine-Westphalia as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of IIJ, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 10 June 2021. The decision on the completeness of the file was taken on 25 June 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of IIJ cover personal data transfers from group members established in the EEA acting as controllers to group members established outside the EEA (Japan, United Kingdom, China, Indonesia, Singapore, Thailand, Vietnam, United States of America) acting as controllers or internal processors, all of which are legally bound by the BCRs as per the Intra-Group-Agreement (see Section 1.2 of the BCRs and Annex 1).
4. Concerned data subjects include employees, suppliers, service providers and customers, including their contact persons (Section 3 of the BCRs)..
5. The draft BCR-C of IIJ have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the IIJ draft BCR-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of IIJ contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁶, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁶ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.⁷

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁷ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 27/2021 on the draft decision of the Supervisory Authority of North Rhine-Westphalia (Germany) regarding the Processor Binding Corporate Rules of the Internet Initiative Japan Group

Adopted on 2 August 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.
- (2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's ("BCR Lead") draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.
- (3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers the EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors, (hereinafter "BCR-P"), including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party,⁴ as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev01. Additionally, WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of the Internet Initiative Japan Group ("IIJ") were reviewed by the Supervisory Authority of North Rhine-Westphalia as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-P of IIJ, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 10 June 2021. The decision on the completeness of the file was taken on 25 June 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-P of IIJ cover personal data transfers from group members established in the EEA to group members established outside the EEA (Japan, United Kingdom, China, Indonesia, Singapore, Thailand, Vietnam, United States of America), all of which acting as processors and being legally bound by the BCRs as per the Intra-Group-Agreement (see Section 1.2 of the BCRs and Annex 1).
4. Concerned data subjects include suppliers, service providers and customers as well as their customers, including in each case their contact persons (see Section 3 of the BCRs).
5. The draft BCR-P of IIJ have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the IIJ draft BCR-P contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing IIJ's Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCRs -P of IIJ contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.⁸

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁸ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 28/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Oregon Tool, Inc (formerly “Blount”)

Adopted on 2 August 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁴ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁵.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Oregon Tools Inc. (formerly "Blount") (hereinafter "Oregon Tool") were reviewed by the Belgian Data Protection Authority as the - Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Oregon Tool requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 24 June 2021. The decision on the completeness of the file was taken on 25 June 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁵ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Oregon Tool cover all processing of personal data within the Oregon Tool Group entities, legally bound by BCR, regardless of the origin of the personal data that Oregon Tool processes, the country in which Oregon Tool processes personal data, or the country in which a group member is established.
4. Concerned data subjects include Oregon Tool past and current employees, individual consultants, independent contractors, temporary staff and job applicants, representatives of businesses customers who use Oregon Tool business services, individual contractors, account managers and staff of third-party suppliers who provide services to Oregon Tool, individuals who visit or register on Oregon Tool's website.
5. The draft BCR-C of Oregon Tool have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Oregon Tool draft BCRs-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Oregon Tool's intra-group agreement on Binding Corporate Rules, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Oregon Tool contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁶, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁶ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.⁷

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁷ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



**Opinion 29/2021 on the draft decision of the Belgian
Supervisory Authority regarding the Processor Binding
Corporate Rules of Oregon Tool, Inc (Formerly “Blount”)**

Adopted on 2 August 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors, (hereinafter "BCR-P"), including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party,⁴ as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev01. Additionally, WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Oregon Tools Inc (Formerly "Blount") (hereinafter "Oregon Tool") were reviewed by the Belgian Data Protection Authority as the - Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-P of Oregon Tool, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 28 May 2021. The decision on the completeness of the file was taken on 25 June 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-P of Oregon Tool cover all processing of personal data within the Oregon Tool Group entities, legally bound by BCR, regardless of the origin of the personal data that Oregon Tool process, the country in which Oregon Tool process personal data, or the country in which a group member is established, when Oregon Tool act as data processors for a third party Controller who is not a group member
4. Concerned data subjects include end users whose personal data an Oregon Tool's customer chooses to share with Oregon Tool for processing.
5. The draft BCR-P of Oregon Tool have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the Oregon Tool draft BCRs-P contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Oregon's Tool's Intra-Group Agreement on Binding Corporate Rules, the EDPB considers that the draft decision of the Belgian Supervisory Authority may be adopted as it is, since the draft BCRs -P of Oregon Tool contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Belgian Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Belgian Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Belgian Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ CJEU, *Data Protection Commissioner v .Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.⁸

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁸ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 30/2021 on the draft decision of the Spanish Supervisory Authority regarding the Controller Binding Corporate Rules of the COLT Group

Adopted on 2 August 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the COLT Group were reviewed by Spanish Supervisory Authority as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of the COLT Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 23 of June 2021. The decision on the completeness of the file was taken on 12 July 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working Party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of the COLT Group cover transfers of personal data when COLT Group entities, legally bound by the BCRs and that have implemented the BCRs, act as Data Controllers or as Data Processors on behalf of another controller of the Group.⁷
4. Concerned data subjects include COLT Group's employees, candidates, officeholders and individuals providing services to COLT as contractors, business contacts at customers or suppliers and Web users⁸.
5. The draft BCR-C of the COLT Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the COLT Group draft BCR-C contain all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the COLT Group's Intra-Company Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of the COLT Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Spanish Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Spanish Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Spanish Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁹, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ BCR-C of COLT, Annex 1, Section 1.1.

⁸ BCR-C of COLT, Annex 1, Section 2.

⁹ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.¹⁰

For the European Data Protection Board

The Chair

(Andrea Jelinek)

¹⁰ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 31/2021 on the draft decision of the Spanish Supervisory Authority regarding the Processor Binding Corporate Rules of the COLT Group

Adopted on 2 August 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors, (hereinafter "BCR-P"), including the Intra-Company Agreement where applicable, and the application form. WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev01. Additionally, WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of the COLT Group were reviewed by the Spanish Supervisory Authority as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-P of the COLT Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 23 of June 2021. The decision on the completeness of the file was taken on 12 July 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working Party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-P of the COLT Group cover transfers of personal data when COLT Group entities, legally bound by the BCRs and having implemented the BCRs, act as Data processors according to the instructions of a non-COLT Data controller established in the EEA.⁷
4. Depending on the services provided to the Data controller, concerned data subjects include Customer's Customers, employees or business contacts⁸.
5. The draft BCR-P of the COLT Group have been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the COLT Group draft BCR-P contain all elements required under Article 47 GDPR and WP257 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the COLT Group's Intra-Company Agreement, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-P of the COLT Group contain appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP 257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the Spanish Supervisory Authority and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the Spanish Supervisory Authority shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the Spanish Supervisory Authority shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁹, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷BCR-P of COLT, Annex 1, Section 1.1.

⁸ BCR-P of COLT, Annex 1, Section 2.

⁹ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU¹⁰.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

¹⁰ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 33/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Carrier

Adopted on 26 October 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the "EDPB") is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter "SA") aims to approve binding corporate rules (hereinafter "BCRs") within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA's (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Carrier was reviewed by the Belgian SA as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Carrier, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 5 July 2021. The decision on the completeness of the file was taken on 15 September 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Carrier covers transfers of personal data by members of Carrier acting as controllers that are legally bound by the BCR-C of Carrier and Intra-group agreement, regardless of where data subjects are located. A number of provisions only apply to personal data originating directly or indirectly from the EEA.
4. Concerned data subjects include employees and outsourced labour (as applicable); job applicants; personnel of suppliers, vendors, and business customers; visitors of Carrier systems and facilities; persons authorised to use Carrier systems; and consumers and end-users of certain Carrier products.
5. The draft BCR-C of Carrier has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of Carrier contains all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-group agreement regarding Binding Corporate Rules, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Carrier contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU⁸.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁸ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 34/2021 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules of Otis

Adopted on 26 October 2021

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	5

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “EDPB”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “SA”) aims to approve binding corporate rules (hereinafter “BCRs”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s (BCRs Lead) draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA, in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

(4) This opinion only covers EDPB's consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs' review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR.

(5) WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter "BCR-C"), including the Intra-Company Agreement where applicable, and the application form. WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev01. Additionally, WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs' national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(6) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(7) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Otis was reviewed by the Belgian SA as the BCR Lead SA (hereinafter the "BCR Lead SA").
2. The BCR Lead SA has submitted its draft decision regarding the draft BCR-C of Otis, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 5 July 2021. The decision on the completeness of the file was taken on 15 September 2021.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

2 ASSESSMENT

3. The draft BCR-C of Otis covers transfers of personal data by members of Otis acting as controllers that are legally bound by the BCR-C of Otis and Intra-group agreement, regardless of where data subjects are located. A number of provisions only apply to personal data originating directly or indirectly from the EEA.
4. Concerned data subjects include employees and outsourced labour (as applicable); job applicants; personnel of suppliers, vendors, and business customers; visitors of Otis systems and facilities; persons authorised to use Otis systems; and consumers and end-users of certain Otis products.
5. The draft BCR-C of Otis has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of Otis contains all elements required under Article 47 GDPR and WP256 rev01, in concordance with the draft decision of the BCR Lead SA submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing Intra-group agreement regarding Binding Corporate Rules, the EDPB considers that the draft decision of the BCR Lead SA may be adopted as it is, since the draft BCR-C of Otis contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data will be transferred to and processed by the group members based in third countries. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

7. This opinion is addressed to the BCR Lead SA and will be made public pursuant to Article 64(5)(b) GDPR.
8. According to Article 64(7) and (8) GDPR, the BCR Lead SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
9. Pursuant to Article 70(1)(y) GDPR, the BCR Lead SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.
10. In accordance with the judgment of the Court of Justice of the European Union C-311/18⁷, it is the responsibility of the data exporter in a Member State, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data

⁷ CJEU, *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, 16 July 2020, C-311/18.

importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU⁸.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

⁸ See EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

Opinion of the Board (Art. 64)



Opinion 39/2021 on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject

Adopted on 14 December 2021

Table of contents

1	INTRODUCTION	3
2	RELEVANT PROVISIONS OF THE GDPR	4
3	SUBJECT MATTER OF THE OPINION.....	5
4	ADOPTED SOLUTION	6

The European Data Protection Board

Having regard to Article 63 and Article 64(2) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 10 and Article 22 of its Rules of Procedure,

Whereas:

(1) The main role of the European Data Protection Board (hereafter the “Board”) is to ensure the consistent application of the GDPR throughout the European Economic Area. Article 64(2) GDPR provides that any supervisory authority, the Chair of the Board or the Commission may request that any matter of general application or producing effects in more than one EEA Member State be examined by the Board with a view to obtaining an opinion. The aim of this opinion is to examine a matter of general application or which produces effects in more than one EEA Member State.

(2) On 6th October 2021, the Hungarian Data Protection Authority requested the Board to examine and issue an opinion on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of personal data, in a situation where such request was not submitted by the data subject.

(3) The opinion of the Board shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authorities have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 INTRODUCTION

1. Each Member States’ supervisory authority is responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to data processing and to facilitate the free flow of personal data within the European Economic Area (“EEA”). In this regard, Article 57(1)(a) GDPR provides that each supervisory authority shall on its territory enforce the application of the GDPR. This duty applies regardless of whether the supervisory authority acts ex officio or on the basis of a complaint. However, in order to carry out this task the supervisory authorities must have effective toolsets, which allow them to take action against infringements of the

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

Regulation. For this reason, Article 58(2) GDPR provides for a set of corrective powers that a supervisory authority can use.

2. As a matter of fact, “*strong enforcement*”, “*consistent and homogenous application of the rules*”, “*equivalent powers for monitoring and ensuring compliance*”, “*equivalent sanctions for infringements*” and “*same tasks and effective powers, including (...) corrective powers*” are all called for by the recitals of the GDPR.²
3. Hence, for the sake of the consistent application of the Regulation by the supervisory authorities, on 6th October 2021, the Hungarian Data Protection Authority requested the Board to examine and issue an opinion on whether Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of unlawfully processed personal data, in a situation where such a request was not submitted by the data subject
4. This question of interpretation concerns a “*matter of general application*” of the GDPR, which has the potential to infringe the fundamental right to data protection. Indeed, the powers conferred upon supervisory authorities by Article 58 GDPR should be interpreted and applied in a consistent manner in order to ensure the consistent application of the GDPR, also in light of the fact that the supervisory authorities’ use of such powers may produce legal effects in more than one Member State (e.g., in the context of One-Stop-Shop procedures).
5. The EDPB has not yet issued guidelines or statements on the matter outlined above. Thus, to enable the consistent application of the GDPR across the EEA, an objective interpretation must be found as to whether or not Article 58(2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of unlawfully processed personal data, in a situation where such request was not submitted by the data subject.

2 RELEVANT PROVISIONS OF THE GDPR

6. Recital 7 GDPR states that due to the rapid technological developments and globalisation “a strong and more coherent data protection framework” is required in the Union, “backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market.”
7. Recital 10 GDPR provides that “In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union.”
8. Recital 11 GDPR states that “Effective protection of personal data throughout the Union requires (...) equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.”
9. Recital 129 GDPR provides that “In order to ensure consistent monitoring and enforcement of this Regulation throughout the Union, the supervisory authorities should have in each Member State the same tasks and effective powers, including powers of investigation, corrective powers and sanctions (...).”

² Recital 7, 10, 11 and 129 GDPR.

10. Article 5(1)(a) and (e) provides that personal data shall be processed lawfully and, as a rule, shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Article 5(2) further enshrines the controller's responsibility to comply with paragraph 1.
11. Chapter VI GDPR, entitled "Independent supervisory authorities", defines the competence, tasks and powers of the data protection authorities in order to contribute to a consistent application GDPR.
12. Article 57(1)(a) GDPR provides that each supervisory authority shall on its territory enforce the application GDPR.
13. Article 58(2)(g) GDPR provides that each supervisory authority shall have the right to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19.
14. Article 17(1) GDPR provides that the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
 - a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
 - c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
 - d) the personal data have been unlawfully processed;
 - e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
 - f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

3 SUBJECT MATTER OF THE OPINION

15. First of all, the Board considers that the consistent application of the corrective powers of the supervisory authorities is of key importance for the consistent level of protection in the European Economic Area.
16. To enable the consistent application and effective implementation GDPR across the EEA, the Board considers that there is a clear need to interpret Article 58(2)(g) GDPR to assess whether it could serve as a legal basis for a supervisory authority to order ex officio the erasure of unlawfully processed personal data in a situation where such request was not submitted by the data subject. In this regard, the supervisory authorities need legal certainty to exercise their powers in a consistent manner, and to avoid the creation of diverging administrative practices on this sensitive subject.
17. The Board underlines, however, that the scope of the opinion is limited to the question raised by the Hungarian Data Protection Authority, hence it only provides clarity on whether Article 58 (2)(g) GDPR could serve as a legal basis for a supervisory authority to order ex officio the erasure of unlawfully processed personal data, in a situation where such request was not submitted by the data subject.

18. The Board emphasises that in the context of this opinion it does not assess the different powers listed in Article 58(2) GDPR, and their interplay. For this reason, the opinion is without prejudice to the other powers listed in Article 58(2) GDPR, and it does not exclude the possibility for supervisory authorities to base their order of erasure on another legal basis provided for in Article 58(2) GDPR.
19. For the Board to be able to assess whether supervisory authorities may order the erasure of personal data under 58(2)(g) GDPR even in the absence of a request for erasure from the data subject, it is essential to assess if Article 17 GDPR imposes an obligation to erase personal data on the controller only following a request from the data subject.
20. Article 17(1) GDPR establishes, on the one hand, the right of the data subject to request the erasure of their personal data and, on the other hand, the obligation of the controller to erase those data where one of the grounds cited in the Article apply. The question that arises is whether this obligation is conditional to the exercise of the right by a data subject, or it exists independently of any request of the data subject.
21. It can be argued that the wording of this Article including its title ("Right of erasure") suggests that the obligation to erase presupposes that the data subject has exercised his/her right to request erasure.
22. However, it can also be argued that Article 17 GDPR provides for both (i) an independent right for data subjects and (ii) an independent obligation for the controller. In this regard, Article 17 GDPR does not require the data subject to take any specific action, it merely outlines that the data subject "has the right to obtain" erasure and the data controller "has the obligation to erase" if one of cases set forth in Article 17(1) GDPR applies.
23. The interpretation that the controller's erasure obligation is independent from the data subject's right for erasure is supported by the fact that some cases set forth in Article 17(1) GDPR clearly refer to scenarios that the controllers must detect as part of their obligation for erasure, independently of whether or not the data subjects are aware of these cases. In fact, it would be difficult for data subjects to be aware of (i) legal obligations to which the controller is subject (letter e); (ii) when the data collected are no longer necessary in relation to the purposes for which they were collected (letter a); or (iii) when personal data are unlawfully processed (letter d). Detecting these circumstances must be the responsibility of the data controllers as part of their compliance with the regulations GDPR, and cannot be the responsibility of the data subjects. This responsibility also stems from Article 5(1) (a), (e) and (2) GDPR.
24. Furthermore, it can be argued that it is of utmost importance for the effective enforcement GDPR, that supervisory authorities possess powerful tools to take efficient actions against infringements. However, an interpretation requiring the prior request for erasure of the data subject for imposing the obligation for erasure on the controller would restrict the supervisory authorities' power in regards to Article 58(2)(g) GDPR.

4 ADOPTED SOLUTION

25. For the Board to assess whether the power of the supervisory authorities under Article 58 (2)(g) GDPR applies even in the absence of a request for erasure from the data subject, it first had to consider whether Article 17 GDPR imposes an obligation on the controller only following a request from the data subject, or if this obligation is independent thereof.

26. In this regard the Board found that Article 17 GDPR provides for two separate cases for erasure that are independent from each other:
 - I. the erasure at the request of the data subject, and
 - II. the erasure as a standalone obligation of the controller.
27. This conclusion of the Board is supported by the fact that some cases set forth in Article 17(1) GDPR clearly refer to scenarios that the controllers must detect on their own as part of their obligation for compliance with the provisions GDPR, and by the rationale to allow supervisory authorities to ensure the enforcement of the principles enshrined in the GDPR even in cases where the data subjects are not informed or aware of the processing, or in cases where not all concerned data subjects have submitted a request for erasure.
28. Based on the above reasoning, the EDPB concludes that Article 58(2)(g) GDPR is a valid legal basis for a supervisory authority to order ex officio the erasure of unlawfully processed personal data in a situation where such request was not submitted by the data subject.
29. This opinion will be made public pursuant to Article 64(5)(b) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 25/2022 regarding the European Privacy Seal
(EuroPriSe) certification criteria for the certification of
processing operations by processors**

Adopted on 13 September 2022

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT	5
2.1	General remarks	5
2.2	Processing operations by a processor	5
2.3	Requirements from a legal perspective.....	5
2.3.1	Record of processing activities	6
2.3.2	Applicants subject to Article 3.2 GDPR	6
2.4	Relationship controller-processor	6
2.5	Requirements for specific types of processing operations.....	8
2.5.1	Statutory confidentiality obligations, professional secrets and special official secrets not based on statutory provisions.....	8
2.5.2	Transfer of personal data to third countries	8
2.6	Data protection by design and by default	9
2.7	Technical and organisational measures	10
2.8	Rights of the data subjects	10
3	CONCLUSIONS / RECOMMENDATIONS	11
4	FINAL REMARKS.....	13

The European Data Protection Board

Having regard to Article 63, Article 64(1)(c) and Article 42 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 64(1)(c) of the GDPR and Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) Member States, supervisory authorities, the European Data Protection Board (hereinafter “the EDPB”) and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms (hereinafter “certification mechanisms”) and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises². In addition, the establishment of certifications can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services³.
- (2) The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of national certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).
- (3) When a supervisory authority (hereinafter “SA”) intends to approve a certification pursuant to Article 42(5) of the GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(1)(c) of the GDPR, the EDPB is required to issue an Opinion on the SA’s draft decision approving the certification criteria.
- (4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation” (hereinafter the “Guidelines”) and their Addendum providing “Guidance on certification criteria assessment” (hereinafter the “Addendum”), for which the public consultation period expired on 26 May 2021.

¹ References to “Member States” made throughout this Opinion should be understood as references to “EEA Member States”.

² Article 42(1) of the GDPR.

³ Recital 100 of the GDPR.

- (5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.
- (6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
- (7) At the same time, the certification criteria should take into account and, where appropriate, be inter-operable with other standards, such as ISO standards, and certification practices.
- (8) As a result, certifications should add value to an organisation by helping to implement standardized and specified organisational and technical measures that demonstrably facilitate and enhance processing operation compliance, taking account of sector-specific requirements.
- (9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.
- (10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.
- (11) The Opinion of the EDPB shall be adopted, pursuant to Article 64(1)(c) of the GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent SA have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.
- (12) The EDPB Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the draft certification criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with Article 42(5) of the GDPR and the Guidelines, the “European Privacy Seal (EuroPriSe) certification criteria for the certification of processing operations by processors” (hereinafter the “draft certification criteria” or “certification criteria”) was drafted by the EuroPriSe Cert GmbH (hereinafter the “EuroPriSe”), a legal entity in Germany and submitted to the Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, the competent German supervisory authority in North Rhine-Westphalia (hereinafter the “DE SA (NRW)”).

2. The DE SA (NRW) has submitted the draft criteria of a national certification scheme to the EDPB and requested an Opinion of the Board pursuant to Article 64(1)(c) GDPR on 2 June 2022. The decision on the completeness of the file was taken on 7 July 2022.

2 ASSESSMENT

3. The Board has conducted its assessment in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter “Annex”) and its Addendum. Where this Opinion remains silent on a specific section of the draft certification criteria, it should be read as the Board not having any comments and not asking the DE SA (NRW) to take further action.

2.1 General remarks

4. In the opinion of the Board, the scope of the certification scheme is not made sufficiently clear. Notwithstanding the fact that the scope of the scheme is indicated between brackets (“(scope: DE)”) on the title page of the document, this page also contains the wording (‘European Privacy Seal’) which may still give the impression that the scheme has a European scope. Therefore, the Board encourages to make the scope of the certification scheme clear in the introductory text of the document.
5. The present certification is not a certification according to Article 46(2)(f) of the GDPR meant for international transfers of personal data. It does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

2.2 Processing operations by a processor

6. In the view of the Board, the assessment whether the applicant is a processor is part of the application review (and not of the criteria pursuant to Article 42(5) of the GDPR). The certification body must assess the role based on the information and documents provided by the applicant when applying for a certification. Therefore, the Board recommends to leave section 1 out of the criteria pursuant to Article 42(5) of the GDPR and incorporate it to the application process.
7. The Board also notes that the current scheme provides for criteria pursuant to Article 28 GDPR to be met in the relationship of the processor with the controller (in section 2.2 of the scheme) and in the relationship of the processor with other processors⁴ (sub processors) (in section 2.3.3 of the scheme). In order to make clear that this does not imply that such sub-processor can be certified under this scheme and that only the processing operations performed on behalf of the applicant is subject to certification, the EDPB recommends to clarify also in the introduction that sub processors cannot be certified under the EuroPriSe certification scheme.

2.3 Requirements from a legal perspective

⁴ Other processors within the meaning of article 28 (2) and (4) of the GDPR.

2.3.1 Record of processing activities

8. The requirement to maintain a record of processing activities pursuant to Article 30 (2) of the GDPR is stipulated in section 2.1.1. of the certification criteria. According to EuroPriSe, this requirement “will be applicable as a rule”. However, the Board encourages to clarify whether the exemptions of Article 30 (5) of the GDPR could still apply in individual cases or if – in order to meet the criteria in the EuroPriSe scheme – such a record of processing activities must always be maintained by a certification customer regardless of the exemptions.

2.3.2 Applicants subject to Article 3.2 GDPR

9. The Board notes that according to section 2.1.3., processors who do not have an establishment in the European Union (EU) or in the European Economic Area (EEA) shall designate a representative in accordance with Article 27 of the GDPR. Consequently, the Board understands that the EuroPriSe certification scheme is applicable for certification customers that are established outside the EU or the EEA.
10. Since this could imply that such a processor established outside the EU/EEA could also process personal data outside the EU/EEA, the Board recommends to clarify in section 2.1.3. that whenever a “transfer” within the meaning of Article 44 of the GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V of the GDPR must be fully respected. Furthermore, the Board recommends to clarify in section 2.1.3. that the present scheme is not a scheme pursuant to Article 46 (2)(f) GDPR. The Board recommends to clarify in section 2.1.3. that the applicant is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46 (2)(f) GDPR. Data controllers should, irrespective of the presence of the certification seal, nonetheless perform an assessment of the legislation of the host country before transferring data to the non-EU GDPR certified processor. In case the legislation does not provide for the appropriate level of protection, supplementary measures should be put in place.⁵
11. A data processor should refrain from applying for certification if they are aware that their legislation would prevent them from complying with the GDPR principles enshrined in the certification scheme.

2.4 Relationship controller-processor

12. The Board notes that under section 2.2 and 2.3 of the EuroPriSe certification criteria, reference is made to the requirements with regard to Article 28 GDPR. Section 2.2.1 of the certification criteria deal with the existence of contractual clauses that meet all the requirements of Article 28 GDPR. In this regard, the Guidance states that the processor draws up a Data Processing Agreement (DPA) template that meets all the requirements of Article 28 GDPR. Notwithstanding the fact that the guidance also mentions that the template does not have to be used, the Board encourages to provide additional wording in this guidance to clarify that such a Data Processing Agreement template is without prejudice to the right of the data

⁵ See EDPB 01/2020 Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: <https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer>.

controller to provide or negotiate the Article 28 GDPR clauses with the data processor without consequences on the certification.

13. Furthermore, section 2.2.1 mentions that this requirement “must be modified if the respective processing by a processor on behalf of the controller is not based on a contract but on another legal instrument under Union or Member State law.” However, when other legal instruments are in place, the requirement of section 2.2.1 is not applicable. In these cases such contractual clauses are not required. The Board recommends to modify the wording accordingly.
14. Section 2.2.1 instructs the Certification Body to examine “whether the relevant legal instrument complies with the requirements of Art. 28 GDPR”, accompanied by a footnote which explains that “this constellation is not considered in more detail in this v2.1 of the criteria catalogue due to lack of practical relevance”. When certain criteria lack practical relevance, they should not be part of the criteria catalogue. The Board therefore recommends to delete these sentences from section 2.2.1.
15. The requirement in section 2.2.1, point 2 e) of the criteria in detail should not just repeat the text of Article 28, but instead the Board recommends to further specify the assistance that the processor should or could offer for the fulfillment of the controller’s obligation to respond to requests for exercising data subject rights. This, in order to reflect the actual operational options the processor and the controller have, i.e. to what extent the controller is practically dependent on the assistance of the controller for the exercise of data subject rights (support being imperative) or the controller merely prefers (some kind of) support from the processor on this issue (support being elective). The requirement should also stipulate that such clauses should be in line with the GDPR responsibility of the controller regarding data subject rights and not unduly transfer this responsibility to the processor.⁶ The EDPB recommends to modify requirement 2.2.1 so that it is taken into account to what extent the controller is actually dependent on the processor for the assistance of the processor regarding data subject rights.
16. Section 2.2.2 (point 8 of the criteria in detail) states that the processor provides all “necessary information” to demonstrate compliance with Article 28 GDPR. It is not completely clear what documents this requirement is specifically referring to, as the list of documents is open ended, and the term “necessary information” rather vague. The Board therefore recommends to identify an exhaustive list of documents/information that has to be checked by the Certification Body to verify if this criteria is fulfilled or not. Furthermore, this criterion should clarify that this documentation/information shall be provided to the Certification Body.
17. Section 2.3.2 states that “the processor shall have concluded contracts with all other processors that impose the same data protection obligations as set out in the contract(s) between the controller(s) and the processor on that other processor”. To enhance readability, the Board encourages to slightly modify the last part of the sentence. For example, “on that other processor” could be changed into “sub-processor”.
18. Section 2.3.2 (point 1a of the requirement in detail) states that the exact time period or the criteria according to which it is determined shall be specified. For reasons of clarity, the Board recommends to include in this requirement that these specifications on the duration of the

⁶ This paragraph should be read this in conjunction with paragraph 35, 36 and 37.

processing shall be in accordance with the relevant provisions of the data processing agreement between the controller and the processor.

2.5 Requirements for specific types of processing operations

2.5.1 Statutory confidentiality obligations, professional secrets and special official secrets not based on statutory provisions

19. The Board notes that the requirement stipulated in section 2.4.1. “is only applicable if the processing operations to be certified are exclusively resp. mainly used by controllers who are subject to special confidentiality / secrecy obligations.” In the view of the Board, it is unclear whether this requirement applies in case only “few” controllers that are subject to special obligations use the processing operations of the certified processor. Furthermore, it is unclear in which circumstances the term “mainly” is fulfilled. Therefore, the Board recommends to clarify section 2.4.1 accordingly.
20. In addition to footnote 63 of the EuroPriSe certification scheme, the Board encourages to provide further examples in the “Guidance” of section 2.4.1. regarding how a contract template for a data processing agreement could address specific confidentiality obligations under EU law or Member State law.⁷

2.5.2 Transfer of personal data to third countries

21. The Board notes that section 2.4.2 stipulates requirements regarding Chapter V of the GDPR. However, the EuroPriSe certification is not itself a transfer instrument for transfers of personal data to third countries or international organisations pursuant to Article 46(2)(f) of the GDPR. In this context, the Board recommends to clarify in section 2.4.2 that the EuroPriSe certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR, as it does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). In addition, the Board recommends to include the obligation of the certification applicant to inform the controller about the fact that the EuroPriSe certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR.
22. Furthermore, the Board recommends to clarify in section 2.4.2 that these specific requirements are only applicable when the certification applicant (as processor) is transferring personal data to a data importer in a third country and to stipulate a requirement for certification applicants to substantiate and document their choice for a particular transfer tool pursuant to Chapter V of the GDPR.
23. Section 2.4.2.1 stipulates general requirements regarding the transfer tools of Chapter V of the GDPR.⁸ In the view of the Board, such general requirements are not auditable and could lead to inconsistencies in the application of the EuroPriSe certification scheme. While there

⁷ The examples could be similar to the “use cases” of section 2.4.2.1.

⁸ « *Here, it SHALL be assessed (and documented) on a case-by-case basis and, as the case may be, in collaboration with the importer (recipient of the personal data in the third country), if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards contained in the transfer tools under Art. 46 GDPR. If this is the case, the processor SHALL implement (and document) supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. In this respect, technical measures, organisational measures and additional contractual measures can be considered, whereby it may be necessary to combine several of these measures in individual cases. »*

are “use cases” to give examples on the application of the EuroPriSe certification scheme, the Board notes that according to EuroPriSe, such “use cases” and “guidance” are not part of the normative criteria. Therefore, this Opinion does not contain conclusions on the correct application of the GDPR in the “use cases” that are provided in section 2.4.2.

24. As a result, since the uses cases address supplementary measures, the Board recommends to include more specifications regarding the assessment of compliance with the data exporter obligations stipulated in Chapter V. In particular, regarding the implementation of supplementary measures, the EDPB Recommendations on measures that supplement transfer tools shall be referred to in the criteria.⁹
25. Finally, the Board notes that section 2.4.2.1. stipulates requirements regarding Article 49 of the GDPR. In this context, the Board recommends to include a requirement of the applicant to provide specific information to the certification body as to which situations and under which conditions the applicant would rely on the exemption of Article 49 of the GDPR.

2.6 Data protection by design and by default

26. Section 2.5.3 states that this requirement does not apply to processing operations by processors that are used by the principals (controllers) for *many* different purposes. The term ‘many’ is too open to be used by a Certification Body to verify conformity. The Board therefore recommends to give more a precise indication of when this requirement is applicable and when it is not, by for instance quantifying the amount of purposes that make it impossible to apply this requirement (for example: “three or more purposes”).
27. In subsection 2.5.3.1 the controller is obliged to use a leaflet which contains information on relevant data protection aspects. Under point 2, it is stated that the leaflet shall contain information on the designation of potential legal bases on which the controller can rely, as the case may be. The Board recommends to delete this point from the criteria catalogue, as it interferes with the responsibility of the controller to define the appropriate legal basis and ensure that all conditions for this legal basis are met. This is without prejudice to the obligation of the processor to immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions, pursuant to Article 28 (3) GDPR.
28. Subsection 2.5.3.1 contains the obligation for the processor to have designated the support services with regard to responding to requests for the exercise of data subject rights in the leaflet. For clarification reasons, and to align with Article 28 (3) (e) GDPR, the Board encourages to modify this sentence as follows: “Designation of the services of the processor with regard to assist the controller in responding to requests for the exercise of data subject rights...”.
29. Subsection 2.5.3.2 contains an obligation to draw up a model form for a declaration of consent or to release from confidentiality if consent is the only legal basis for the use of the processing operations to be certified. The same obligation applies if the processing operations to be certified involve a transfer of personal data to third countries and if consent serves as the legitimization for said transfer. Although such a model might be helpful for some controllers, in

⁹ See EDPB 01/2020 Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data <https://edpb.europa.eu/our-work-tools/our-documents/recommendations-recommendations-012020-measures-supplement-transfer>.

particular small and medium sized enterprises, the Board recommends to delete this specific requirement, as acquiring consent is not the responsibility of the processor but of the controller, and thus cannot serve as a criteria for the processor to demonstrate compliance with the GDPR, which, in the end, is the purpose of GDPR certification.

2.7 Technical and organisational measures

30. The Board notes that referring to the risk analysis in section 3.1.1.1. and 3.1.5.1, it is not entirely clear which risks are being addressed (e.g. those of the data subjects). The Board therefore recommends specifying that the risks to the rights and freedoms of the data subjects are addressed. Furthermore, the document refers in the guidelines of several requirements to a classification of risks, however, in none of the requirements a clarification of this classification has been made. For the sake of clarity, the Board therefore recommends adding in Section 3.1.1.1 and Section 3.1.5.1 a reference to the classification of risks regarding the different types of risks with regard to the data subjects concerned.
31. In section 3.1.1.3, the Board acknowledges the intention of EuroPriSe to highlight the importance of implementing access control mechanisms when interacting with web-based services. However, the current wording "*this is particularly ensured when interacting with web-based services*" might indicate that these control mechanisms are not as important or obligatory in all other cases. The Board therefore encourages to either delete this sub sentence or rephrase it accordingly.
32. The requirement in section 3.1.2.1. stipulates the processor's obligation to demonstrate that "the storage duration of the log data can be configured resp. is actually configured in consideration of the existing resp. assumed risk". However, the Board notes that according to Article 5 (1)(c) of the GDPR, the storage duration needs to be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is being processed. The Board therefore encourages adding a reference to consider not only the risks but the purpose of the processing as well.
33. The Board furthermore notes that the "Requirement in a nutshell" in section 3.1.2.1 and section 3.1.2.2. are identical, although the requirements "in detail" deal with different aspects. For the sake of clarity, the Board encourages to consider this differentiation in the "*requirements in a nutshell*" as well.

2.8 Rights of the data subjects

34. As a consequence of the recommendations made by the Board on sections 2.2.1 and 2.2.2 pertaining to contractual clauses on the assistance to be provided by the processor to the controller to facilitate the exercise of data subjects rights, the Board also recommends to reflect and take into account such relevant differences in the contractual clauses in Chapter IV of the EuroPriSe scheme. Also the Board recommends to modify the same approach reflected in the requirements (4.1-4.8) for all the data subjects rights (4.2-4.8), generally phrased as an obligation for the processor to implement 'technical and organizational measures' without any further specification of such measures. Such modifications should reflect the significant differences in the various data subjects' rights, since some of those rights will always be applicable (a), some will depend on a further legal assessment of the situation (b) and some will depend on a substantial appreciation (c). Consequently

responsibilities of the controller and the processor pertaining to (b) and (c) will have to be clarified in the contractual clauses.

35. The requirement in section 4.1 is unspecific as to ‘which information is relevant with regards to the controllers’ information obligations towards data subjects’ that shall be provided by the processor. The Board recommends a further specification taking into account the elements mentioned in Articles 13 and 14 of the GDPR.
36. Regarding the requirement in section 4.8, the Board considers that the controller is in charge of deciding the purposes and means of the processing, and it would therefore appear to be out of the sphere of the responsibility of a processor. Therefore, the Board recommends to further specify which kind of support the processor should provide with regards to the exercise of the right not to be subjected to a decision based solely on automated processing, including profiling.

3 CONCLUSIONS / RECOMMENDATIONS

37. By way of conclusion, the EDPB considers that the EuroPriSe certification criteria may lead to an inconsistent application of the GDPR and the following changes need to be made in order to fulfill the requirements imposed by Article 42 of the GDPR in light of the Guidelines and the Addendum:

38. regarding the “scope of the scheme”, the Board recommends:

- 1) to leave out section 1 of the criteria pursuant to Article 42(5) of the GDPR and incorporates it to the application process.
- 2) to clarify in the introduction that sub processors cannot be certified under the EuroPriSe certification scheme.

39. regarding the “applicants subject to Article 3.2 GDPR”, the Board recommends:

- 1) to include a reminder in section 2.1.3. that whenever a “transfer” within the meaning of Article 44 of the GDPR to a processor established outside the EU or the EEA takes place, the obligations stipulated in Chapter V of the GDPR must be fully respected.
- 2) to clarify in section 2.1.3. that the present scheme is not a scheme pursuant to Article 46 (2)(f) of the GDPR.
- 3) to clarify in section 2.1.3. that the applicant is not entitled to make use of the certification in a way that could give the impression that the certification itself is a transfer tool pursuant to Article 46 (2)(f) GDPR.

40. regarding the “relationship controller-processor”, the Board recommends:

- 1) to adjust the wording of the requirement of section 2.2.1 so that it is clear that when other legal instruments are in place, the requirement of Section 2.2.1 is not applicable.
- 2) to delete sentences in section 2.2.1 with regard to a “lack of practical relevance”.

- 3) to modify requirement 2.2.1 so that it is taken into account to what extent the controller is actually dependent on the processor for the assistance of the processor regarding data subject rights.
- 4) to identify an exhaustive list of documents in section 2.2.2 (point 8 of the requirement in detail) that has to be checked by the Certification Body to verify if this criteria is fulfilled or not. Furthermore, this criterion should clarify that this information shall be provided to the Certification Body.
- 5) to include in section 2.3.2 (point 1a of the requirement in detail) that the specifications on the duration of the processing shall be in accordance with the relevant provisions of the data processing agreement between the controller and the processor.

41. regarding the “statutory confidentiality obligations, professional secrets and special official secrets not based on statutory provisions”, the Board recommends:

- 1) to include an explanation of the term “mainly used by controllers” in section 2.4.1.

42. regarding the “transfer of personal data to third countries”, the Board recommends:

- 1) to include a reminder in section 2.4.2 that the EuroPriSe certification scheme itself is not a certification according to Article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2).
- 2) to include the obligation of the certification applicant to inform the controller about the fact that the EuroPriSe certification scheme itself is not a transfer instrument according to Article 46(2)(f) of the GDPR.
- 3) to clarify in section 2.4.2 that these requirements are only applicable when the certification applicant (as processor) is transferring personal data to a data importer in a third country and to stipulate a requirement for certification applicants to substantiate and document their choice of a particular transfer tool pursuant to Chapter V of the GDPR.
- 4) to include more specifications regarding the assessment of compliance with the data exporter obligations stipulated in Chapter V. In particular, regarding the implementation of supplementary measures, the EDPB Recommendations on measures that supplement transfer tools shall be referred to in the criteria.
- 5) to include the requirement in Section 2.4.2 that the certification applicant must provide specific information to the certification body in which situations and under which conditions he would rely on the exemption of Article 49 of the GDPR.

43. regarding data protection by design and by default, the Board recommends:

- 1) to give more a precise indication of when the requirement of section 2.5.3 is applicable.

- 2) to delete from the criteria catalogue in subsection 2.5.3.1 under point 2, the part in which is stated that the leaflet shall contain information on the designation of potential legal bases on which the controller can rely.
- 3) to delete from subsection 2.5.3.2 the obligation to draw up a model form for a declaration of consent or to release from confidentiality if consent is the only legal basis for the use of the processing operations to be certified.

44. regarding “technical and organisational measures”, the Board recommends:

- 1) to specify in section 3.1.1.1. and section 3.1.5.1 that the risks to the rights and freedoms of the data subjects are addressed.
- 2) to include in section 3.1.1.1 and section 3.1.5.1 a reference to the classification of risks regarding the different types of risks with regard to the data subjects concerned.

45. Regarding the rights of data subjects, the Board recommends:

- 1) to reflect and take into account such relevant differences with regard to the assistance of the processor (see recommendations on sections 2.2.1 and 2.2.2) in the contractual clauses in Chapter IV of the EuroPriSe scheme.
- 2) to modify the same approach reflected in the requirements (4.1-4.8) for all the data subjects rights (4.2-4.8), generally phrased as an obligation for the processor to implement ‘technical and organizational measures’ without any further specification of such measures.
- 3) to further specify requirement 4.1 (right to information) taking into account the elements mentioned in Articles 13 and 14 of the GDPR.
- 4) to further specify which kind of support the processor should provide in requirement 4.8.

4 FINAL REMARKS

46. This Opinion is addressed to the DE SA (NRW) and will be made public pursuant to Article 64(5)(b) of the GDPR.
47. According to Article 64(7) and (8) of the GDPR, the DE SA (NRW) shall communicate its response to this Opinion to the Chair by electronic means within two weeks after receiving the Opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the Opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this Opinion, in whole or in part.
48. The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the DE SA (NRW) shall make public the certification criteria in an easily accessible form, and transmit them to the Board for inclusion in the public register of certification mechanisms and data protection seals, as per Article 42(8) of the GDPR.

For the European Data Protection Board
The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 18/2022 on the draft decision of the Baden-Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Daimler Truck Group

Adopted on 26 August 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Daimler Truck AG and its controlled group companies (hereinafter the “**Daimler Truck Group**”) was reviewed by the Baden-Württemberg (Germany) SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Daimler Truck Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 8 June 2022. The decision on the completeness of the file was taken on 4 July 2022.

2 ASSESSMENT

3. The draft BCR-C of the Daimler Truck Group covers the processing of personal data:
 - a) from Daimler Truck Group Companies and their subsidiaries that are established in the EEA,
 - b) from Daimler Truck Group Companies established outside the EEA, if they offer goods or services to natural persons within the EEA and/or monitor the behaviour of natural persons within the EEA or
 - c) of Daimler Truck Group Companies established outside the EEA, if they have received personal data directly or indirectly from companies that are subject to the BCR-C of the Daimler Truck Group under a) or b), or if such data has been disclosed to them⁷.
4. Concerned data subjects include employees, prospective customers, customers, drivers, partners, suppliers⁸.
5. The draft BCR-C of the Daimler Truck Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Daimler Truck Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Data Protection Agreement for IL Governance Functions*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Daimler Truck Group contains

⁷ Section 2 of the BCR-C.

⁸ Annex 2 (General description of data transmissions to third countries) of the BCR-C.

appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 19/2022 on the draft decision of the Baden-Württemberg (Germany) Supervisory Authority regarding the Controller Binding Corporate Rules of the Mercedes-Benz Group

Adopted on 26 August 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Mercedes-Benz Group AG⁷ and its controlled group companies (hereinafter “**Mercedes-Benz Group**”) was reviewed by the Baden-Württemberg (Germany) SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Mercedes-Benz Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 8 June 2022. The decision on the completeness of the file was taken on 4 July 2022.

2 ASSESSMENT

3. The draft BCR-C of the Mercedes-Benz Group covers the processing of personal data:
 - a) from Mercedes-Benz Group Companies and their subsidiaries that are established in the EEA,
 - b) from Mercedes-Benz Group Companies established outside the EEA, if they offer goods or services to natural persons within the EEA and/or monitor the behaviour of natural persons within the EEA or
 - c) of Mercedes-Benz Group Companies established outside the EEA, if they have received personal data directly or indirectly from companies that are subject to the BCR-C of the Mercedes-Benz Group under a) or b), or if such data has been disclosed to them⁸.
4. Concerned data subjects include employees, prospective customers, customers, partners, and suppliers⁹.
5. The draft BCR-C of the Mercedes-Benz Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Mercedes-Benz Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Data Protection Agreement for IL Governance Functions*, the EDPB considers that the draft decision

⁷ Formerly Daimler AG.

⁸ Section 2 of the BCR-C.

⁹ Annex 2 (General description of data transmissions to third countries) of the BCR-C.

of the BCR Lead may be adopted as it is, since the draft BCR-C of the Mercedes-Benz Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 20/2022 on the draft decision of the Irish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ellucian Group

Adopted on 26 August 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Ellucian Ireland Limited and its entities (hereinafter the “**Ellucian Group**”) was reviewed by the Irish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Ellucian Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 2 June 2022. The decision on the completeness of the file was taken on 4 July 2022.

2 ASSESSMENT

3. The draft BCR-C of the Ellucian Group covers the processing of personal data by Ellucian Group members legally bound by the BCRs, when they act as controllers or as processors on behalf of another controller of the Ellucian Group⁷ and they apply to all transfers of personal data within the Ellucian Group⁸.
4. Concerned data subjects include Ellucian Group’s job applicants; current and former employees and their families, dependents, beneficiaries and emergency contact persons; current and former personnel and staff and vendors / contractors of current and prospective customers, partners, vendors, third-party suppliers and contractors; and website visitors⁹.
5. The draft BCR-C of the Ellucian Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Ellucian Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Intra-Company Adoption Agreement For Controller Binding Corporate Rules (BCR-C) And Processor Binding Corporate Rules (BCR-P)*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Ellucian Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The

⁷ Ellucian Group BCR-C, Rule 4.1 and Annex 5 (Data Processing Particulars).

⁸ Ellucian Group BCR-C, Rule 4.2 and Annex 5 (Data Processing Particulars)..

⁹ Ellucian Group BCR-C , Rule 4.1 and Annex 5 (Data Processing Particulars).

EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 21/2022 on the draft decision of the Irish Supervisory Authority regarding the Processor Binding Corporate Rules of the Ellucian Group

Adopted on 26 August 2022

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Ellucian Ireland Limited and its entities (hereinafter the “**Ellucian Group**”) was reviewed by the Irish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Ellucian Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 2 June 2022. The decision on the completeness of the file was taken on 4 July 2022.

2 ASSESSMENT

3. The draft BCR-P of the Ellucian Group covers the processing of personal data by Ellucian Group members legally bound by the BCRs, when they act as processors on behalf of a non-Ellucian Group controller established in the EU⁷ and they will geographically apply as determined by the relevant controller⁸.
4. Concerned data subjects include Ellucian Group’s customers’ current and former (a) students, (b) prospective students, (c) parents or benefactors of students or prospective students, (d) alumni, (e) faculty members, (f) administration, (g) employees, (h) prospective employees, (i) vendors / contractors / agents, and (j) donors⁹.
5. The draft BCR-P of the Ellucian Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Ellucian Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Ellucian Group BCR-P, Rule 4.1 and Annex 4 (Data Processing Particulars).

⁸ Ellucian Group BCR-P, Rule 4.2.

⁹ Ellucian Group BCR-P, Rule 4.1 and Annex 4 (Data Processing Particulars).

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Intra-Company Adoption Agreement For Controller Binding Corporate Rules (BCR-C) And Processor Binding Corporate Rules (BCR-P)*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Ellucian Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 22/2022 on the draft decision of the Liechtenstein Supervisory Authority regarding the Controller Binding Corporate Rules of Hilti Group

Adopted on 7 September 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Hilti Aktiengesellschaft and its entities (hereinafter the “**Hilti Group**”) was reviewed by the Liechtenstein SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Hilti Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 5 July 2022. The decision on the completeness of the file was taken on 18 August 2022.

2 ASSESSMENT

3. The draft BCR-C of the Hilti Group covers the processing of personal data by the Hilti Group entities bound by the BCR-C⁷.
4. Concerned data subjects include customers; contact persons; suppliers; job applicants and candidates; current and former employees; and employees’ dependents for the purpose of insurance, pension, social security benefits allowance and employee mobility purposes⁸.
5. The draft BCR-C of the Hilti Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Hilti Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Binding Corporate Rules Joining Agreement*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Hilti Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

⁷ Hilti Group BCR-C, section 2.a. Geographical scope and Appendix 2 - Hilti Entities.

⁸ Hilti Group BCR-C, section 2.b. Material scope and Appendix 3 - Binding Corporate Rules Material Scope.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 23/2022 on the draft decision of the Swedish Supervisory Authority regarding the Controller Binding Corporate Rules of the Samres Group

Adopted on 7 September 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Samres AB and the members of the Samres Group (hereinafter the “**Samres Group**”) was reviewed by the Swedish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Samres Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 29 June 2022. The decision on the completeness of the file was taken on 18 August 2022.

2 ASSESSMENT

3. The draft BCR-C of the Samres Group covers the processing of personal data from Samres Group members legally bound by the BCR-C acting as controllers or as processors on behalf of another controller of the Samres Group, and they apply to all transfers of personal data within the Samres Group⁷.
4. Concerned data subjects include employees, prospective employees, business partner representatives, stakeholder representatives, civil servants at authorities, and other third parties the Samres Group may interact with (e.g., office visitors, trainees or journalists)⁸.
5. The draft BCR-C of the Samres Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Samres Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Samres Group BCR-C*, designed as an intra-group agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Samres Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs.

⁷ Section 1.2 of the BCR-C.

⁸ Section 4.1 of the BCR-P and its Appendix 2, Section 2.1.

Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 24/2022 on the draft decision of the Swedish Supervisory Authority regarding the Processor Binding Corporate Rules of the Samres Group

Adopted on 7 September 2022

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Samres AB and the members of the Samres Group (hereinafter “**Samres Group**”) was reviewed by the Swedish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Samres Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 29 June 2022. The decision on the completeness of the file was taken on 18 August 2022.

2 ASSESSMENT

3. The draft BCR-P of the Samres Group covers all transfers of personal data, regardless of the origin of the personal data, whenever Samres Group members legally bound by the BCR-P are acting as processors or sub-processors on behalf of a controller outside of the Samres Group⁷.
4. Concerned data subjects include the users of the services they perform on behalf of their customers (i.e., travellers and their representatives); drivers and other transport personnel, administrative personnel at other companies and authorities, as well as other third parties that the Samres Group may interact with on behalf of the Samres Group’s customers (e.g., trainees, office visitors or journalists)⁸.
5. The draft BCR-P of the Samres Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Samres Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Samres Group BCR-P*, designed as an intra-group agreement, the EDPB considers that the draft

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Sections 1.2 and 1.4 of the BCR-P.

⁸ Section 4.1 of the BCR-C and its Appendix 2, Section 2.2.

decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Samres Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 26/2022 on the draft decision of the Data Protection Authority of Bavaria for the Private Sector regarding the Controller Binding Corporate Rules of the Munich Re Reinsurance Group

Adopted on 30 September 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München and its group members (hereinafter “**Munich Re Reinsurance Group**”) was reviewed by the Data Protection Authority of Bavaria for the Private Sector as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Munich Re Reinsurance Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 22 July 2022. The decision on the completeness of the file was taken on 18 August 2022.

2 ASSESSMENT

3. The draft BCR-C of the Munich Re Reinsurance Group covers the transfer, including the subsequent processing, of EEA personal data⁷ by or on behalf of Munich Re Reinsurance Group members within the EEA to Munich Re Reinsurance Group members in third countries⁸.
4. Concerned data subjects include current, former or prospective representatives and employees of Munich Re Reinsurance Group members, representatives, employees and contact persons at current, former or prospective corporate customers, and current, former or prospective customers of primary insurers/cedents⁹.
5. The draft BCR-C of the Munich Re Reinsurance Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Munich Re Reinsurance Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement regarding the Binding Corporate Rules for the Processing of EEA Data by Munich Re Reinsurance Group Members, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Munich Re Reinsurance Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the

⁷ In this context, “EEA personal data” refers to personal data that are or have been processed on behalf of a Munich Re Reinsurance Group Member within the EEA and, therefore, has been subject to the GDPR.

⁸ Section 2 of the BCR-C.

⁹ Annex 2 (Section 26.1) of the BCR-C.

GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 27/2022 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of LEYTON Group

Adopted on 7 October 2022

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Thésée (the holding company of the Leyton group) and its entities (hereinafter “**Leyton Group**”) was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Leyton Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 21 July 2022. The decision on the completeness of the file was taken on 18 August 2022.

2 ASSESSMENT

3. The draft BCR-P of the Leyton Group apply when a Leyton entity acts as a data processor for and according to the instructions of a non-Leyton data controller established in the EEA. They apply to BCR entities established in an EEA country exporting personal data directly or indirectly, and to BCR entities not established in an EEA country importing the personal data. They cover first transfers of personal data and onward transfers. They do not apply to transfers of personal data between entities located in adequate third countries or EEA member states, or to entities located in an adequate third country or EEA Member State⁷.
4. Concerned data subjects include the staff of the clients (employees, temporary workers, interns, etc.); the contractual partners of the clients or their representatives, and their prospective clients, if any; and the third parties involved with regard to the services (particularly, the court officers, court-appointed representatives, etc.)⁸.
5. The draft BCR-P of the Leyton Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Leyton Group contains all elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Articles 1 and 4.2 of the BCR.

⁸ Article 5.4 of the BCR.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Commitment of conformity, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Leyton Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



**Opinion 28/2022 on the Europrivacy criteria of certification
regarding their approval by the Board as European Data
Protection Seal pursuant to Article 42.5 (GDPR)**

Adopted on 10 October 2022

The European Data Protection Board

Having regard to Article 63, Article 64(2) and Article 42 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Articles 10 and 22 of its Rules of Procedure.

- (1) Member States, supervisory authorities, the European Data Protection Board (hereinafter “the EDPB or the Board”) and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms(hereinafter “certification mechanisms”) and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises.² In addition, the establishment of certification mechanisms can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services.³
- (2) The criteria of certification form an integral part of a certification mechanism. Consequently, the GDPR requires the approval of the criteria of a national certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).
- (3) When a supervisory authority (hereinafter “SA”) intends to propose the approval by the EDPB of a European data protection seal pursuant to article 42(5) of the GDPR, the SA should state the intention of the scheme owner to offer the certification mechanism in all Member States. In this case, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(2) of the GDPR, the EDPB is approving the criteria of certification.
- (4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements, which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation” (hereinafter the “Guidelines”) and their Addendum providing “Guidance on certification criteria assessment” (hereinafter the “Addendum”), for which the public consultation period expired on 26 May 2021.
- (5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.

¹ References to “Member States” made throughout this Opinion should be understood as references to “EEA Member States”.

² Article 42(1) of the GDPR.

³ Recital 100 of the GDPR.

- (6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR. Therefore, its criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
- (7) At the same time, scheme owner should ensure the alignment and conformity of the certification mechanism with any included or leveraged ISO standards and certification practices.
- (8) As a result, certifications should add value to controllers and processors by helping to implement standardized and specified organizational and technical measures that demonstrably facilitate and enhance processing operation compliance to the GDPR, taking account of sector-specific requirements.
- (9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.
- (10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent supervisory authorities from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.
- (11) In this Opinion, the EDPB addresses issues, such as the scope of the criteria, the applicability and relevance of the criteria in all Member States.
- (12) This Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.
- (13) The Opinion of the EDPB shall be adopted, pursuant to Article 64(2) of GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter. If the opinion of the EDPB concludes that the criteria cannot be approved at stake, the SA may resubmit the criteria for approval when the concerns expressed in the initial EDPB Opinion are addressed.

HAS ADOPTED THE FOLLOWING OPINION:

SUMMARY OF THE FACTS

1. In accordance with Article 42(5) of the GDPR and the Guidelines, the Europrivacy v.60 criteria (hereinafter the “draft certification criteria”, “certification criteria” or “criteria”) was drafted by European Center for Certification and Privacy (hereinafter the “scheme owner”).
2. The Supervisory Authority of Luxembourg (hereinafter the “LU SA”) has submitted the Europrivacy criteria of certification to the EDPB for approval pursuant to Article 64(2) GDPR on 28 September 2022. The decision on the completeness of the file was taken on 28 September 2022.
3. The Europrivacy certification mechanism is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international

organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

2 ASSESSMENT

4. The EDPB has conducted its assessment of the criteria of certification for their approval under Articles 42(5) of the GDPR in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter “Annex”) and its Addendum.
5. The EDPB notes that the implementing guidance and suggested means of verification of the certification mechanism provided by the scheme owner are not always consistent throughout the catalogue of criteria. For instance, section T.2.3.2 requires that rules, policies, procedures or mechanisms are in place to detect and report intrusions (e.g. an intrusion detection system that monitors network traffic for suspicious activity and alerts when such activity is discovered), whereas the suggested means of verification refer to inspection and penetration test (required in section T.2.3.1). Although such inconsistencies do not fall under the scope of its assessment, the EDPB underlines that they may be a barrier to the accreditation of the certification body, unless rectified by the scheme owner.

2.1 Scope of the certification mechanism and Target of Evaluation (ToE)

6. The Europrivacy certification mechanism is a general scheme in that it targets a large range of different processing operations performed by controllers and processors from various sectors of activity. The main criteria of this certification mechanism are composed of the “Core criteria” and of the “TOMs checks and controls” concerning technological and organisational measures set in place to secure the processed personal data. A set of the “TOMs checks and controls” criteria are only applicable if the Target of Evaluation (hereinafter “ToE”) processes special categories of data, criminal offense related data, or personal data of a child.
7. Additionally, the criteria also include “Complementary contextual checks and controls” that aim to ensure that the data processing involved in the ToE comply with domain-specific and technology-specific requirements. An informative matrix provided by the scheme owner describes to which categories of data processing operations, each set of the “Complementary contextual checks and controls” criteria apply.
8. The EDPB welcomes general schemes that include specific criteria so to make them scalable and applicable to specific processing operations or sector of activity. However, the EDPB also wishes to clarify that in the context of a general scheme, the completeness of the criteria relating to specific processing operations is not required and thus was not assessed in the context of this Opinion. In addition, the EDPB recalls that when it publishes documents related to specific processing activities, such documents shall be taken into account by the scheme owner and the accredited certification bodies.
9. The criteria applicable to the specification of the ToE are defined in the requirements available in A.2.1.1. The specific rules applicable to the process to be followed by the applicant and by the certification body in order to define the ToE are specified by the Europrivacy scheme (10.2 - Pre-certification Activities).

10. The Board notes in the documentation related to the scope of the certification mechanism provided by LU SA that the Europrivacy scheme applies to controllers and processors established in the European Union (EU) or in the European Economic Area (EEA). The applicability of the criteria is defined depending on the role and responsibilities of the applicant
11. The Board notes that a data controller can submit to the Europrivacy certification process a ToE which is subject to joint-controllership (criteria A.2.7.1). In case the ToE is subject to joint-controllership, the Board wishes to underline that the accredited certification body will have to carefully conduct the application process to ensure that the ToE is meaningful and that the applicant is fully responsible for the compliance of the ToE with all obligations under the GDPR that the certification mechanism aims at demonstrating. As a consequence, the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the obligations under the GDPR⁴ might – depending on the context of the processing activities of the ToE - prevent the applicant to fulfil the criteria of certification.
12. The Board notes that the data processing of genetic data is excluded from the scope of the Europrivacy certification mechanism. As a consequence, the assessment of the criteria conducted by the Board does not cover the suitability of the criteria for ToE that would include such data processing.

2.2 Processing operations

13. The criteria address the relevant components of the processing operations (data, systems, and processing) with respect to the general scope of the certification mechanism. In particular, the criteria allow identifying special categories of data as defined in Article 9 of the GDPR (section G.2 of the criteria - Special Data Processing).

2.3 Lawfulness of processing

14. The criteria require checking the lawfulness of the data processing for each individual processing operations in the ToE and require checking the requirements of a legal basis as defined in Article 6 of the GDPR (section G.1 of the criteria - Lawfulness of Data Processing).

2.4 Principles of data processing

15. The criteria adequately address the data protection principles pursuant to Article 5 of the GDPR. In particular, the criteria require the applicant to demonstrate that the personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

2.5 General obligations of controllers and processors

16. The criteria reflect the obligations of the controller pursuant to article 24 of the GDPR (G.4 - Data Controller Responsibility) and require the evaluation of processor-controller contractual agreements

⁴ *The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities (Guidelines 07/2020 on the concepts of controller and processor in the GDPR)*

in accordance with Article 28 of the GDPR (section G.5 of the criteria - Data Processors or sub Processors).

17. The criteria require all applicants to appoint a Data Protection Officer (DPO) even in the case where the applicant is not required to designate a DPO according to Article 37 of the GDPR. The criteria check that the DPO meet the requirements under Articles 37 to 39 (section G.9 of the criteria - Data Protection Officer).
18. The criteria check the content of the records of processing of activities in accordance with Article 30 of the GDPR (section G.5.3 of the criteria - Records of processing activities).

2.6 Rights of the data subjects

19. The criteria adequately address data subject's right to information in accordance with Chapter III of the GDPR and require respective measures to be put in place. The criteria also require measures put in place providing for the possibility to intervene in the processing operation in order to guarantee data subjects' rights and allow corrections, erasure or restrictions (section G.3 of the criteria - Rights of the Data Subjects).

2.7 Risks for the rights and freedom

20. The criteria require assessing the risk to the rights and freedoms of natural persons of the data processing involved in the ToE in accordance with Article 35 of the GDPR (section G.8 of the criteria - Data Protection Impact Assessment).

2.8 Technical and organisational measures guaranteeing protection

21. The criteria require the application of technical and organisational measures providing for confidentiality, integrity and availability of processing operations. The criteria also require the application of technical measures to implement data protection by design and by default in accordance with Article 25 and Article 32 of the GDPR (section G.6 of the criteria - Security of Processing and Data Protection by Design, Section T.1/T.2 of the criteria – Core Security Requirements/Extended Security Requirements).
22. The criteria require the application of measure to ensure that personal data breach notification duties are carried out in due time and scope in accordance with Article 33 and 34 of the GDPR (section G.7 of the criteria - Management of Data Breaches).

2.9 Criteria for the purpose of demonstrating the existence of appropriate safeguards for transfer of personal data

23. The criteria require identifying all personal data transfers to third countries and to international organizations involved in the ToE and substantiating the choice made regarding the data transfer mechanism providing for appropriate safeguards, pursuant to Chapter V of the GDPR (section G.10 of the criteria - Transfers of personal data to third countries or international organisations).

3. ADDITIONAL CRITERIA FOR A EUROPEAN DATA PROTECTION SEAL

24. According to the Guidelines, the assessment shall include the question on "whether the criteria are able to take into account Member State data protection laws or scenarios". Section G.1.1.3 of the criteria requires the applicant to provide such an assessment in a National Obligations Compliance Assessment Report (NOCAR). The Board notes that such report shall include an assessment of the

national obligations applicable to the ToE and will document the measures taken by the applicant to comply with applicable rules and, possibly, ongoing corrective actions. The applicant shall not use the key complementary national requirements list provided by the scheme owner for each country as an exhaustive list of national obligations relevant for the ToE. The indicative list of minimal complementary checks and controls requirement provided by the scheme owner are not criteria of certification in the scope of this Opinion.

CONCLUSIONS / RECOMMENDATIONS

25. By way of conclusion, the EDPB considers that the Europrivacy criteria of certification are consistent with the GDPR and approves them pursuant to the task of the Board defined in article 70(1)(o) of the GDPR, resulting in a common certification (European Data Protection Seal).
26. The EDPB will register the Europrivacy certification mechanism in the public register of certification mechanisms and data protection seals and marks pursuant to Article 42(8).

FINAL REMARKS

27. This Opinion is addressed to the LU SA and will be made public pursuant to Article 64(5)(b) of the GDPR.

For the European Data Protection Board

The Chair

Opinion of the Board (Art. 64)



Opinion 29/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the DSV Group

Adopted on 18 November 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of DSV A/S and its group entities (hereinafter the “**DSV Group**”) was reviewed by the Danish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the DSV Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 4 October 2022. The decision on the completeness of the file was taken on 18 October 2022.

2 ASSESSMENT

3. The draft BCR-C of the DSV Group covers the processing by DSV Group Members of personal data originating from the EEA⁷.
4. Concerned data subjects include current and former employees of DSV Group Members, including their emergency contacts/next of kind; job applicants; customers, suppliers and business partners of the DSV Group; consignees; visitors to websites and social media accounts of DSV Group Members; shareholders⁸.
5. The draft BCR-C of the DSV Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the DSV Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the “Agreement regarding processing and transfer of Personal Data under DSV’s BCR”, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the DSV Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third

⁷ Section 3.1 of the BCR-C.

⁸ Section 3.3.1 of the BCR-C and Appendix 1.

countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 30/2022 on the draft decision of the Slovak Supervisory Authority regarding the Controller Binding Corporate Rules of Piano Group

Adopted on 28 November 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of PIANO SOFTWARE GROUP and its affiliates (hereinafter “**Piano Group**”) was reviewed by the Slovak SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Piano Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 12 August, 2022. The decision on the completeness of the file was taken on 4 October 2022.

2 ASSESSMENT

3. The draft BCR-C of Piano Group covers the processing by BCR Members acting as joint controllers of personal data transferred, directly or indirectly, from the EEA to third countries as well as to: (i) any subsequent processing of personal data by BCR Members in such third countries, and; (ii) any subsequent onward transfers to or sub-processing of non-Piano Group (external) entities⁷.
4. Concerned data subjects include employees or potential employees of Piano Group’s members, employees of Piano Group’s service providers and advisors, representatives or contact persons of Piano Group’s suppliers or business partners, visitors of Piano Group’s websites or social media profiles⁸.
5. The draft BCR-C of the Piano Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Piano Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Piano’s *Group Data Processing Agreement*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Piano Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific

⁷ Sections 1.1. and 1.2 of the Piano BCR-C.

⁸ Section 5.5. of the Piano BCR-C; Section 8 of the Group Data Processing Agreement.

transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 31/2022 on the draft decision of the Slovak Supervisory Authority regarding the Processor Binding Corporate Rules of Piano Group

Adopted on 28 November 2022

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS / RECOMMENDATIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the WP265 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of PIANO SOFTWARE GROUP and its affiliates (hereinafter “Piano Group”) was reviewed by the Slovak SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Piano Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 12 August 2022. The decision on the completeness of the file was taken on 4 October 2022.

2 ASSESSMENT

3. The draft BCR-P of the Piano Group covers the processing of personal data by Piano Group members legally bound by the BCRs, when they act as processors or sub-processors on behalf of a non-Piano Group controller established in the EEA. The BCR-P will apply to the processing of personal data transferred, directly or indirectly, from the EEA to third countries as well as to: (i) any subsequent processing of personal data by BCR Members in such third countries; and; (ii) any subsequent onward transfers to or sub-processing of non-Piano Group (external) entities⁷.
4. Concerned data subjects include any type of data subject pursuant to the data processing agreement or instruction of Piano Group's clients, mainly online users or visitors of websites, applications or online services of clients towards which Piano Group's services are directed⁸.
5. The draft BCR-P of the Piano Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Piano Group contains all elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Section 1.1 and 1.2 of the Piano Group BCR-P.

⁸ Section 5.5 of Piano Group BCR-P.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Piano's *Group Data Processing Agreement*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Piano Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 32/2022 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Ramboll Group

Adopted on 6 December 2022

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Ramboll Group A/S and its participating corporate entities (hereinafter the “**Ramboll Group**”) was reviewed by the Danish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Ramboll Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 17 October 2022. The decision on the completeness of the file was taken on 31 October 2022.

2 ASSESSMENT

3. The draft BCR-C of the Ramboll Group covers the processing of personal data transferred directly or indirectly out of the EEA to any of the Ramboll Group members⁷.
4. Concerned data subjects include current and former employees of Ramboll Group members, including consultants; job applicants; customers; subcontractors; suppliers and other business contacts⁸.
5. The draft BCR-C of the Ramboll Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Ramboll Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the “Data Protection Binding Corporate Rules Undertaking”, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Ramboll Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

⁷ Section 3 of the BCR-C.

⁸ Section 3 and Appendix 7 of the BCR-C.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 6/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of Royal Greenland Group

Adopted on 23 March 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Royal Greenland A/S and its entities, factories, offices or other business subsidiaries⁷ (hereinafter “**Royal Greenland Group**”) was reviewed by the Danish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Royal Greenland Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 28 November 2022. This request was withdrawn on 15 February 2023 and re-submitted the same day, including an additional document following exchanges with the EDPB Secretariat. The decision on the completeness of the file was taken on 22 February 2023.

2 ASSESSMENT

3. The draft BCR-C of Royal Greenland Group covers the processing of personal data transferred directly or indirectly out of the EEA to any of the Royal Greenland Group members⁸.
4. Concerned data subjects include potential, current and former employees; business customers, suppliers, and other business partners⁹.
5. The draft BCR-C of the Royal Greenland Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Royal Greenland Group contains all elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Agreement regarding Royal Greenland BCRs, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Royal Greenland Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval

⁷ Section 3.1 of the BCR-C.

⁸ Section 2.2 of the BCR-C and Appendix 2.

⁹ Section 1.2 of the BCR-C and Appendix 1.

of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

Opinion of the Board (Art. 64)



Opinion 11/2023 on the draft decision of the competent supervisory authority of Sweden regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 11 July 2023

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	4
2.1	General reasoning of the Board regarding the submitted draft accreditation requirements.	4
2.2	Analysis of the SE SA's accreditation requirements for Code of Conduct's monitoring bodies	
	5	
2.2.1	GENERAL REMARKS.....	5
2.2.2	INDEPENDENCE.....	6
2.2.3	CONFLICT OF INTEREST	6
2.2.4	EXPERTISE.....	7
2.2.5	ESTABLISHED PROCEDURES AND STRUCTURES	7
2.2.6	TRANSPARENT COMPLAINT HANDLING	7
2.2.7	COMMUNICATION WITH THE SE SA	7
2.2.8	REVIEW MECHANISMS.....	8
2.2.9	LEGAL STATUS.....	8
2.2.10	SUBCONTRACTING	8
3	CONCLUSIONS / RECOMMENDATIONS.....	8
4	FINAL REMARKS.....	9

The European Data Protection Board

Having regard to Article 63, Article 64 (1)(c), (3)-(8) and Article 41 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and Article 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the European Data Protection Board (hereinafter “the Board”) is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter “SA”) intends to approve the requirements for accreditation of a code of conduct (hereinafter “code”) monitoring body pursuant to article 41. The aim of this opinion is therefore to contribute to a harmonised approach with regard to the suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a code monitoring body by the competent supervisory authority. Even though the GDPR does not directly impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinion by: firstly, requesting the competent SAs to draft their requirements for accreditation of monitoring bodies based on article 41(2) GDPR and on the Board’s “Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679” (hereinafter the “Guidelines”), using the eight requirements as outlined in the guidelines’ accreditation section (section 12); secondly, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs to adopt the requirements in line with this opinion, so as to achieve an harmonised approach.

(2) With reference to article 41 GDPR, the competent supervisory authorities shall adopt requirements for accreditation of monitoring bodies of approved codes. They shall, however, apply the consistency mechanism in order to allow the setting of suitable requirements ensuring that monitoring bodies carry out the monitoring of compliance with codes in a competent, consistent and independent manner, thereby facilitating the proper implementation of codes across the Union and, as a result, contributing to the proper application of the GDPR.

(3) In order for a code covering non-public authorities and bodies to be approved, a monitoring body (or bodies) must be identified as part of the code and accredited by the competent SA as being capable of effectively monitoring the code. The GDPR does not define the term “accreditation”. However, article 41 (2) of the GDPR outlines general requirements for the accreditation of the monitoring body. There are a number of requirements, which should be met in order to satisfy the competent supervisory authority to accredit a monitoring body. Code owners are required to explain and

¹ References to the “Union” made throughout this opinion should be understood as references to “EEA”.

demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

(4) While the requirements for accreditation of monitoring bodies are subject to the consistency mechanism, the development of the accreditation requirements foreseen in the Guidelines should take into consideration the code's sector or specificities. Competent supervisory authorities have discretion with regard to the scope and specificities of each code, and should take into account their relevant legislation. The aim of the Board's opinion is therefore to avoid significant inconsistencies that may affect the performance of monitoring bodies and consequently the reputation of GDPR codes of conduct and their monitoring bodies.

(5) In this respect, the Guidelines adopted by the Board will serve as a guiding thread in the context of the consistency mechanism. Notably, in the Guidelines, the Board has clarified that even though the accreditation of a monitoring body applies only for a specific code, a monitoring body may be accredited for more than one code, provided it satisfies the requirements for accreditation for each code.

(6) The opinion of the Board shall be adopted pursuant to article 64 (3) GDPR in conjunction with article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Swedish Supervisory Authority (hereinafter "SE SA") has submitted its draft decision containing the accreditation requirements for a code of conduct monitoring body to the Board, requesting its opinion pursuant to article 64 (1)(c), for a consistent approach at Union level. The decision on the completeness of the file was taken on 16 May 2023.

2 ASSESSMENT

2.1 General reasoning of the Board regarding the submitted draft accreditation requirements

2. All accreditation requirements submitted to the Board for an opinion must fully address article 41 (2) GDPR criteria and should be in line with the eight areas outlined by the Board in the accreditation section of the Guidelines (section 12, pages 21-25). The Board opinion aims at ensuring consistency and a correct application of article 41 (2) GDPR as regards the presented draft.
3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

4. All codes covering non-public authorities and bodies are required to have accredited monitoring bodies. The GDPR expressly request SAs, the Board and the Commission to “encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium sized enterprises.” (article 40 (1) GDPR). Therefore, the Board recognises that the requirements need to work for different types of codes, applying to sectors of diverse size, addressing various interests at stake and covering processing activities with different levels of risk.
5. In some areas, the Board will support the development of harmonised requirements by encouraging the SA to consider the examples provided for clarification purposes.
6. When this opinion remains silent on a specific requirement, it means that the Board is not asking the SE SA to take further action.
7. This opinion does not reflect upon items submitted by the SE SA, which are outside the scope of article 41 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Analysis of the SE SA’s accreditation requirements for Code of Conduct’s monitoring bodies

8. Taking into account that:
 - a. Article 41 (2) GDPR provides a list of accreditation areas that a monitoring body need to address in order to be accredited;
 - b. Article 41 (4) GDPR requires that all codes (excluding those covering public authorities per Article 41 (6)) have an accredited monitoring body; and
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for monitoring bodies and conduct the accreditation of a body for monitoring codes of conduct.

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board observes that the SE SA’s draft accreditation requirements sometimes refer to an obligation (“shall”) and sometimes to a possibility (“should”). For the sake of clarity, the Board recommends that the SE SA avoid the use of “should” in the text of the accreditation requirements.
10. For the sake of consistency, the Board encourages the SE SA to adjust the terminology used in the requirements to the ones used in the Guidelines, this applies in particular to the following terms:
 - in section 4.9, reference should be made to “data processing in scope of the code” and “complaints received or specific incidents”;
 - in sections 5.7 and 5.10, reference should be made to “corrective measures” instead of “measures”;
 - in section 8.3, it should be referred to “monitoring body and related governance structures”.

11. The SE SA's draft accreditation requirements state in the introduction that an internal monitoring body "could be an internal department within the code owner or an ad hoc internal committee". The Board considers that it should be made explicit that an internal monitoring body cannot be setup within a code member. Therefore, the Board recommends adding a relevant requirement.
12. The Board notes that, in the section dedicated to the duration of accreditation, the reference to review does not mention that the SE SA will review the compliance with the requirements periodically. Thus, the Board encourages the SE SA to specify the possible duration of the accreditation (for example in years or for an indefinite period of time), to clarify that the requirements may be reviewed periodically and to provide transparent information on how the periodic review will work in practice and what happens after the expiry of the validity of the accreditation.

2.2.2 INDEPENDENCE

13. Having examined section 1.1.3, the Board acknowledges that the SE SA states that "the duration or expiration of the mandate of the monitoring body must be regulated in such a way to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely effects the independence in carrying out the monitoring activities by the Monitoring body." The Board is of the opinion that this requirement would benefit from the inclusion of additional explanation on what duration could lead to adverse effects on the independence of the monitoring body. Therefore, the Board encourages the SE SA to include a requirement that the duration of the term of the monitoring body should be indicated.
14. With regard section 1.1.5, the Board encourages the SE SA to delete the word "undue" as a monitoring body must be free not only from "undue" but from any external pressure or influence.
15. Regarding example h) under Section 1.1.4 of the SE SA's draft accreditation requirements, the Board encourages the SE SA to clarify the terms "associations/organisation submitting the code of conduct" by making a reference to "other relations between the monitoring body and not only the code owner but also the members of the code".
16. The Board considers that, in particular in the case of an internal monitoring body, the monitoring body must prove full autonomy for the management of the budget or other resources. Accordingly, the Board recommends that the SE SA replace the term "could" by "must" in section 1.2.1.
17. The Board considers that monitoring bodies must have sufficient financial and other resources together with the necessary procedures to ensure the functioning of the code of conduct over time. This is why, with respect to section 1.2.3 of the draft requirements, the Board encourages the SE SA to add a clear indication that financial stability and resources need to be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time.
18. As regard section 1.3.3 of the SE SA's draft accreditation requirements the Board encourages the SE SA to clarify that demonstration that the monitoring body is composed of an adequate and proportionate number of personnel could be made through procedures to appoint the monitoring body personnel, the remuneration of the said personnel, as well as the duration of the personnel's mandate, contract or other formal agreement with the monitoring body. In addition, The Board encourages the SE SA to redraft the relevant part of the requirements by adding a reference to "adequate and proportionate number of sufficiently qualified personnel".

2.2.3 CONFLICT OF INTEREST

19. The Board encourages the SE SA to clarify in section 2.1 that the staff chosen by the monitoring body or other body should be "independent of the code member".

20. In addition, in section 2.4, the Board encourages the SE SA to clarify that not only procedures but also “measures” to deal with the effects of situations identified as being likely to create a conflict of interest should be provided.

2.2.4 EXPERTISE

21. The Board notes that SE SA’s draft accreditation requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. Therefore, the Board encourages the SE SA to clarify in section 3 which requirement should be met by the staff performing the monitoring function and the personnel making the decisions.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

22. Furthermore, the Board considers that the examples in section 4.3 could be further substantiated, in accordance with paragraph 72 of the Guidelines, by referring to the different ways in which such investigations can be conducted, such as random or unannounced audits, annual inspections, regular reporting and the use of questionnaires. Therefore, the Board encourages the SE SA to redraft the requirement, to make clear that the audit can be carried out in different ways.
23. Moreover, the Board notes that section 4.4 refers to the obligation for monitoring bodies to establish ad hoc procedures to actively and effectively monitor the code members’ compliance with the code’s provisions. In order to ensure consistency with the wording used in section 4.2 the Board encourages the SE SA to amend the wording to refer to “upfront, ad hoc and regular procedures”.

2.2.6 TRANSPARENT COMPLAINT HANDLING

24. According to section 5.10, the monitoring body *could* make information concerning any sanctions leading to suspension or exclusion of code members – and any subsequent lifting hereof – publicly available. Without prejudice to national legislation, the Board encourages the SE SA to replace the term “could” by “must” and to amend this requirement to provide that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate.
25. The Board notes that section 5.7 of the SE SA’s draft accreditation requirements refers to the obligation for monitoring bodies to inform the SA of the measures taken and the reasons for taking them. In line with paragraph 77 of the Guidelines, the Board recommends that the SE SA amend this requirement in order to clarify that this notification should also be made to “the competent SA and, where required, all concerned SAs”.

2.2.7 COMMUNICATION WITH THE SE SA

26. With regard to section 6 of the SE SA’s draft accreditation requirements, the Board recommends that the SE SA make reference to the effective communication with other competent supervisory authorities and not only with the SE SA, as far as transnational codes are concerned.
27. The Board understands that section 6.2 of the requirements refers to the information that the monitoring body will provide to the SE SA upon request. The Board is of the opinion that the requirement to communicate “any actions” need to address such areas as: actions taken in cases of infringement of the code and the reasons for taking them (article 41 (4) GDPR), periodic reports, reviews or audit findings. Therefore, the Board encourages the SE SA to clarify this requirement accordingly.

2.2.8 REVIEW MECHANISMS

28. As regards section 7.3, the Board is of the opinion that the monitoring body should be able to contribute to reviews of the code as required by the code owner and shall therefore ensure that it has documented plans and procedures to review the operation of the code to ensure that the code remains relevant to the members and continues to adapt to any changes in the application and interpretation of the law and new technological developments. Therefore, the Board encourages the SE SA to reflect in the text that both changes in the application and interpretation of the law and/or new technological developments need to always be taken into consideration.

2.2.9 LEGAL STATUS

29. In section 8.2, the Board encourages the SE SA to specify that capability of being held legally responsible for monitoring activities should include that fines per Article 83(4)(c) GDPR can be imposed on the monitoring body and met.
30. In section 8.5, the Board encourages the SE SA to make a clear connection between the first and the second sentence of this section. In addition, the Board encourages the SE SA to clarify that, in order to demonstrate the continuity of the monitoring function, the monitoring body should demonstrate that it has sufficient financial and other resources, and the necessary procedures.
31. With respect to section 8.6, the Board agrees with the SE SA that a natural person must demonstrate adequate resources that allow it to act as a monitoring body. The Board encourages the SE SA to specify how in case of natural persons the necessary expertise (legal and technical) is ensured and to add a clear reference to the necessity of ensuring and documenting how the monitoring role is guaranteed over a long term and how it can deliver the code's monitoring mechanism over a suitable period of time.

2.2.10 SUBCONTRACTING

32. As regards section 9 of the SE SA's draft accreditation requirements, the Board encourages the SE SA to add the reference to compliance. Moreover, the Board encourages the SE SA to include a clear requirement for subcontractors to comply with their data protection obligations.
33. In section 9.2, the Board recommends that the SE SA add a clear indication that the monitoring body shall ensure effective monitoring of the services provided by the contracting entities. Moreover, the Board underlines the need to specify requirements relating to the termination of the contract, in particular so as to ensure that the subcontractors fulfil their data protection obligations, and encourages the SE SA to add such requirement.

3 CONCLUSIONS / RECOMMENDATIONS

34. The draft accreditation requirements of the Swedish Supervisory Authority may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:
35. Regarding *general remarks* the Board recommends that the SE SA:
1. avoid the use of "should" in the text of the accreditation requirements.
 2. make explicit that an internal monitoring body cannot be setup within a code member.
36. Regarding *independence* the Board recommends that the SE SA:
1. replace the term "could" by "must" in section 1.2.1.

37. Regarding *transparent complaint handling* the Board recommends that the SE SA:
 1. amend section 5.7 in order to clarify that this notification should also be made to "the competent SA and, where required, all concerned SAs"
38. Regarding *communication with the SE SA* the Board recommends that the SE SA:
 1. make reference in section 6 to the effective communication with other competent supervisory authorities and not only with the SE SA, as far as transnational codes are concerned
39. Regarding *subcontracting* the Board recommends that the SE SA:
 1. add a clear indication that the monitoring body shall ensure effective monitoring of the services provided by the contracting entities.

4 FINAL REMARKS

40. This opinion is addressed to the Swedish supervisory authority and will be made public pursuant to Article 64 (5) (b) GDPR.
41. According to Article 64 (7) and (8) GDPR, the SE SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
42. The SE SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 12/2023 on the draft decision of the competent supervisory authority of Cyprus regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 11 July 2023

Table of contents

1	Summary of the Facts	4
1.1	General reasoning of the EDPB regarding the submitted draft decision.....	4
1.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
1.2.1	PREFIX.....	6
1.2.2	GENERAL REMARKS.....	6
1.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION.....	6
1.2.4	RESOURCE REQUIREMENTS.....	7
1.2.5	PROCESS REQUIREMENTS	7
1.2.6	MANAGEMENT SYSTEM REQUIREMENTS.....	8
2	Conclusions / Recommendations	8
3	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Cypriot (hereinafter “CY SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 16 May 2023. The CY national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria pursuant to Article 43 GDPR. This means that the NAB will use ISO 17065 and the additional requirements set up by the CY SA, once they are approved by the CY SA, following an opinion from the Board on the draft requirements, to accredit certification bodies. The accreditation will be issued by the NAB after a favorable opinion provided by the CY SA according to the national law.³

1.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the CY SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation. To this end, the CY SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

³ Law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data, Law 125(I)/2018)

3. This assessment of CY SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.
4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the CY SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the CY SA to take further action.
8. This opinion does not reflect upon items submitted by the CY SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.
9. This Opinion does not reflect upon the terms of cooperation of the CY SA with the NAB, as included in the "Prefix" Section of CY SA's draft accreditation requirements.

1.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
 - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
 - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
 - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
 - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

1.2.1 PREFIX

11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

1.2.2 GENERAL REMARKS

12. The Board notes that there are some typos throughout the text of the CY SA's draft accreditation requirements (e.g. section 3, 2016/679/EC instead of (EU)) and thus encourages the CY SA to ensure that such typos will be corrected as appropriate.
13. The Board notes that the CY SA, in some parts of the draft requirement, makes use of the term "should" instead of "shall". The Board encourages the CY SA to replace the term "should" with "shall" so to ensure that the requirements are mandatory as appropriate, taking into account the Guidelines. As an example, this change should be made in section 4.1.2 of the draft accreditation requirements, number 9.

1.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

14. With respect to section 4.1.1. of the CY SA's draft accreditation requirements "the certification body shall be able to demonstrate evidence of the GDPR compliance at any time during the accreditation

process”. At the sentence right above it is mentioned “As the certification body is a data controller/processor itself, it shall be able to demonstrate evidence of the GDPR and Law 125(I)/2018 compliant procedures and measures specifically for controlling and handling of client organization’s personal data as part of the certification process”. To avoid confusion and repetition, the Board encourages the CY SA to remove the first sentence from the requirements.

15. Regarding the consistency of the terminology, the Board encourages the CY SA to use the term “requirement(s)” consistently throughout the text (e.g. section 6.2. to replace the term “conditions” with the term “requirement”) so to avoid confusion.

1.2.4 RESOURCE REQUIREMENTS

16. Regarding section 6.1 “certification body personnel” and in particular the personnel with technical expertise, the Board takes note of the insertion of “Must have obtained a degree in information technology, computer science or mathematics of at least EQF level 6 from a Cypriot, Greek or a foreign university or an equivalent vocational education enjoying a recognized protected title in the Member State where it was issued”. The Board recommends that the CY SA to amend this requirement, by replacing the term “degree” with the term “qualification” in order to bring it line with the Guidelines.
17. With respect to the same paragraph of this section, the Board recommends the CY SA to align the wording with this of the Guidelines. In particular, the Board recommends the CY SA, to add, in addition to the “relevant professional experience”, that this experience must also be significant.
18. In section 6.1., concerning personnel with legal expertise, the CY SA mentions “Personnel responsible for certification decisions shall demonstrate at least two years of professional and comprehensive experience and expertise in certification measures related to data protection law”. The Board encourages the CY SA to re-draft this requirement to reflect that the experience and expertise are related to the sector of certification measures with regards to data protection law.
19. In addition, in the same section (bullet point 3), the Board recommends the CY SA, in order to bring this requirement in line with the Guidelines, to replace the term “technical” procedures with the term “comparable”.

1.2.5 PROCESS REQUIREMENTS

20. In section 7.1, point 3 the CY SA states “that certification bodies have established procedures to examine that the procedures and mechanisms of the applicant for processing and handling personal data related to the scope of the certification and the ToE are compliant with the GDPR;” The Board understands that the terms “scope of certification” and “ToE” have the same meaning, thus the Board encourages the CY SA to delete one of the two terms so to avoid confusion.
21. Concerning point 4 of the same section, the Board encourages the CY SA to delete the word “requested” before the word certification so to avoid confusion.
22. Regarding section 7.2 “application” of the draft accreditation requirements, the Board takes note of the fact that the certification body shall provide a short description to the CY SA of each one of the applications. The Board welcomes this insertion, however it encourages the CY SA to clarify that what this short description what the CY SA wants to receive entails.

23. As regards to section 7.11 “termination, reduction, suspension or withdrawal of certification” the CY SA refers to non-compliance with the certification in case of grave data breach incidents relating to the scope of the certification and the ToE. The Board understands by this requirement that in case that a significant data breach, related with the scope of the certification and the ToE, occurs, which indicates, by its nature, that the client had not taken appropriate measures as expected according to its certification, in the sense that , if the relevant certification requirements were indeed properly implemented, such a data breach would not have been occurred, then this should be considered as non-compliance with the certification, and appropriate actions should be taken by the certification body. The Board encourages the CY SA to clarify in its accreditation requirement.

1.2.6 MANAGEMENT SYSTEM REQUIREMENTS

24. With respect to section 8 of the CY SA’s draft accreditation requirements, the CY SA refers to the Guidelines “These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and at the request of the Office of CPDP at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) of the GDPR or a review of the certifications issued in accordance with Article 42(7) of the GDPR pursuant to Article 58(1)(c) of the GDPR”. The Board notes that the part of the sentence stating that “the accredited certification body pursuant in the accreditation procedure pursuant to Article 58” is reflected in the Guidelines, but this requirement, as stands, creates confusion. To this purpose, the Board recommends the CY SA to delete this part of the sentence.

2 CONCLUSIONS / RECOMMENDATIONS

25. The draft accreditation requirements of the Cypriot Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
26. Regarding ‘resource requirements’, the Board recommends that the CY SA:
- 1) amend the requirement in section 6.1, by replacing the term “degree” with the term “qualification” in order to bring it line with the Guidelines.
 - 2) add in section 6.1, on top of the “relevant professional experience”, that this experience must also be significant.
 - 3) replace in section 6.1 (bullet 3), the term “technical” procedures with the term “comparable”.
27. Regarding ‘management system requirements’, the Board recommends that the CY SA:
- 1) remove, in section 8, the part of the sentence stating that “the accredited certification body pursuant in the accreditation procedure pursuant to Article 58” so to avoid creating confusion.

3 FINAL REMARKS

28. This opinion is addressed to the Cypriot Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
29. According to Article 64 (7) and (8) GDPR, the CY SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
30. The CY SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 13/2023 on the draft decision of the competent supervisory authority of Croatia regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 11 July 2023

Table of contents

1	Summary of the Facts	4
2	Assessment	4
2.1	General reasoning of the EDPB regarding the submitted draft decision.....	4
2.2	Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:	5
2.2.1	PREFIX.....	6
2.2.2	GENERAL REMARKS.....	6
2.2.3	GENERAL REQUIREMENTS FOR ACCREDITATION.....	6
2.2.4	RESOURCE REQUIREMENTS.....	7
2.2.5	PROCESS REQUIREMENTS	7
3	Conclusions / Recommendations	7
4	Final Remarks	8

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,¹

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

¹ References to the "Union" made throughout this opinion should be understood as references to "EEA".

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.²

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Croatian (hereinafter “HR SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 16 May 2023. The HR national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the HR SA, once they are approved by the HR SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the HR SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.
3. This assessment of HR SA’s additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB’s

² Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.
5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.
6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.
7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the HR SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the HR SA to take further action.
8. This opinion does not reflect upon items submitted by the HR SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.
9. This Opinion does not reflect upon the terms of cooperation of the HR SA with the NAB, as included in the "Prefix" Section of HR SA's draft accreditation requirements.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

- a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.
- b. independence of the certification body
- c. conflicts of interests of the certification body
- d. expertise of the certification body
- e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body
- f. procedures for issuing, periodic review and withdrawal of GDPR certification; and
- g. transparent handling of complaints about infringements of the certification.

10. Taking into account that:
- a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;
 - b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;
 - c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;
 - d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);
 - e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;
 - f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

[2.2.1 PREFIX](#)

11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

[2.2.2 GENERAL REMARKS](#)

12. With respect to section 1 “scope” of the HR SA’s draft accreditation requirements, there is a reference to “The broad scope of ISO 17065 covering products, processes and services should not lower or override the requirements of the GDPR, e.g. a governance mechanism cannot be the only element of a certification mechanism, as the certification must include processing of personal data, i.e. the processing operations.” The Board acknowledges the fact that this wording come from the Guidelines. However, it encourages the HR SA to replace the word “should” with “shall” in order to make it clear that the ISO 17065 must not lower or override the GDPR requirements.

[2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION](#)

13. Regarding section 4.2 “management of impartiality” the Board acknowledges the insertion by the HR SA of the requirement to prevent conflicts of interest. However, the Board encourages the HR SA to also include in the accreditation requirements rules to manage conflicts of interests, when such conflicts have been identified.

2.2.4 RESOURCE REQUIREMENTS

14. With respect to section 6.1 “certification body personnel” of HR SA’s draft accreditation requirements and in particular the personnel with technical expertise, the Board takes note of the insertion of “Must have obtained a degree in information technology, computer science or mathematics of at least EQF3 level 6 from a Croatian or a foreign university [...].” The Board recommends that the HR SA amends this requirement, by replacing the term “degree” with the term “qualification” in order to bring it line with the Guidelines.
15. The Board under section 6.2 of the draft accreditation requirements notes that the evaluation activities can be outsourced to external bodies. Thus, the Board recommends the HR SA to clarify in this section that even when such activities are outsourced, the certification body will retain the responsibility for the decision-making.

2.2.5 PROCESS REQUIREMENTS

16. With regards to section 7.2 “application” of HR SA’s draft accreditation requirements, bullet point 4, the Board recommends the HR SA to bring this in line with the text of the Guidelines.
17. With respect to section 7.10 of the draft accreditation requirements and the relevant reference to the “decisions of the European Data Protection Board”, the Board acknowledges that the HR SA has used the wording foreseen in Annex 1. However, in order to ensure a clear understanding of what is meant by “decisions of the European Data Protection Board”, the Board encourages the HR SA to clarify the reference. An example could be to refer to “documents or publications adopted by the European Data Protection Board”

3 CONCLUSIONS / RECOMMENDATIONS

18. The draft accreditation requirements of the HR Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
19. Regarding ‘resource requirements’, the Board recommends that the HR SA:
 - 1) amend this requirement, by replacing the term “degree” with the term “qualification” in order to bring it line with the Guidelines.
 - 2) clarify in section 6.2 that even when evaluation activities are outsourced, the certification body will retain the responsibility for the decision-making.
20. Regarding ‘process requirements’, the Board recommends that the HR SA:
 - 1) With regards to section 7.2 “application” of HR SA’s draft accreditation requirements, bullet point 4, the Board recommends the HR SA to bring this in line with the text of the Guidelines.

³ See qualifications framework comparison tool at: <https://europa.eu/europass/en/compare-qualifications>

4 FINAL REMARKS

21. This opinion is addressed to the Croatian Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
22. According to Article 64 (7) and (8) GDPR, the HR SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list or where it does not intend to follow the opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this opinion, in whole or in part.
23. The HR SA shall communicate the final decision to the Board for inclusion in the register of decisions, which have been subject to the consistency mechanism, in accordance with article 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 14/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Vestas Wind Systems Group

Adopted on 27 July 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP256 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. Additionally, the WP264 informs the applicants that any documentation submitted is subject to access to documents requests in accordance with the SAs’ national laws. The EDPB is subject to Regulation 1049/2001⁵ pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Vestas Wind Systems A/S and its subsidiaries and affiliates (hereinafter the “**Vestas Group**”) was reviewed by the Denmark SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Vestas Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 12 May 2023. The decision on the completeness of the file was taken on 6 June 2023.

2 ASSESSMENT

3. The draft BCR-C of the Vestas Group covers the intra-group transfers of personal data to third countries by members of the Vestas group.⁷
4. Concerned data subjects include job applicants, employees, and employees of customers, business partners and suppliers processed internally by the Vestas Entities.⁸
5. The draft BCR-C of the Vestas Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Vestas Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement annexed to the BCR-C, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Vestas Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

⁷ Vestas BCR Policy, p. 2: *What data does the BCR cover?*

⁸ Vestas BCR Policy, p.2: *What data does the BCR cover?* and Appendix 7.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Adopted

Opinion of the Board (Art. 64)



**Opinion 15/2023 on the draft decision of the Dutch
Supervisory Authority regarding the Brand Compliance
certification criteria**

Adopted on 19 09 2023

Table of contents

1	SUMMARY OF THE FACTS.....	4
2	ASSESSMENT.....	5
3	CONCLUSIONS / RECOMMENDATIONS.....	14
4	FINAL REMARKS.....	16

The European Data Protection Board

Having regard to Article 63, Article 64(1)(c) and Article 42 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “GDPR”),

Having regard to the European Economic Area (hereinafter “EEA”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 64(1)(c) of the GDPR and Articles 10 and 22 of its Rules of Procedure.

Whereas:

- (1) Member States, supervisory authorities, the European Data Protection Board (hereinafter “the EDPB”) and the European Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms (hereinafter “certification mechanisms”) and of data protection seals and marks, for the purpose of demonstrating compliance with the GDPR of processing operations by controllers and processors, taking into account the specific needs of micro, small and medium-sized enterprises². In addition, the establishment of certifications can enhance transparency and allow data subjects to assess the level of data protection of relevant products and services³.
- (2) The certification criteria form an integral part of any certification mechanism. Consequently, the GDPR requires the approval of national certification criteria of a certification mechanism by the competent supervisory authority (Articles 42(5) and 43(2)(b) of the GDPR), or in the case of a European Data Protection Seal, by the EDPB (Articles 42(5) and 70(1)(o) of the GDPR).
- (3) When a supervisory authority (hereinafter “SA”) intends to approve a certification pursuant to Article 42(5) of the GDPR, the main role of the EDPB is to ensure the consistent application of the GDPR, through the consistency mechanism referred to in Articles 63, 64 and 65 of the GDPR. In this framework, according to Article 64(1)(c) of the GDPR, the EDPB is required to issue an Opinion on the SA’s draft decision approving the certification criteria.
- (4) This Opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors in the light of the core elements which certification mechanisms have to develop. In particular, the EDPB assessment is carried out on the basis “Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation” (hereinafter the “Guidelines”) and their Addendum providing “Guidance on certification criteria assessment” (hereinafter the “Addendum”), for which the public consultation period expired on 26 May 2021.

¹ References to “Member States” made throughout this Opinion should be understood as references to “EEA Member States”.

² Article 42(1) of the GDPR.

³ Recital 100 of the GDPR.

- (5) Accordingly, the EDPB acknowledges that each certification mechanism should be addressed individually and is without prejudice to the assessment of any other certification mechanism.
- (6) Certification mechanisms should enable controllers and processors to demonstrate compliance with the GDPR; therefore, the certification criteria should properly reflect the requirements and principles concerning the protection of personal data laid down in the GDPR and contribute to its consistent application.
- (7) At the same time, the certification criteria should take into account and, where appropriate, be inter-operable with other standards, such as ISO standards, and certification practices.
- (8) As a result, certifications should add value to an organisation by helping to implement standardized and specified organisational and technical measures that demonstrably facilitate and enhance processing operation compliance, taking account of sector-specific requirements.
- (9) The EDPB welcomes the efforts made by scheme owners to elaborate certification mechanisms, which are practical and potentially cost-effective tools to ensure greater consistency with the GDPR and foster the right to privacy and data protection of data subjects by increasing transparency.
- (10) The EDPB recalls that certifications are voluntary accountability tools, and that the adherence to a certification mechanism does not reduce the responsibility of controllers or processors for compliance with the GDPR or prevent SAs from exercising their tasks and powers pursuant to the GDPR and the relevant national laws.
- (11) The Opinion of the EDPB shall be adopted, pursuant to Article 64(1)(c) of GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks from the first working day after the Chair and the competent SA have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.
- (12) The EDPB Opinion focusses on the certification criteria. In case the EDPB requires high level information on the evaluation methods in order to be able to thoroughly assess the auditability of the draft certification criteria in the context of its Opinion thereof, the latter does not encompass any kind of approval of such evaluation methods.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with Article 42(5) of the GDPR and the Guidelines, the “Brand Compliance certification standard” (hereinafter the “draft certification criteria” or “certification criteria”) was drafted by Brand Compliance B.V. (hereinafter “Brand Compliance”), a legal entity in the Netherlands and submitted to the Dutch SA (hereinafter the “NLSA”).
2. The NL SA has submitted its draft decision approving the Brand Compliance certification criteria, and requested an Opinion of the EDPB pursuant to Article 64(1)(c) GDPR on 26 April 2023. The decision on the completeness of the file was taken on 4 July 2023.

2 ASSESSMENT

3. The Board has conducted its assessment in line with the structure foreseen in Annex 2 to the Guidelines (hereinafter “Annex”) and its Addendum. Where this Opinion remains silent on a specific section of the Brand Compliance’s draft certification criteria, it should be read as the Board not having any comments and not asking the NL SA to take further action.
4. The present certification is not a certification according to article 46(2)(f) of the GDPR meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in letter (f) of Article 46(2). Indeed, any transfer of personal data to a third country or to an international organisation, shall take place only if the provisions of Chapter V of the GDPR are respected.

2.1 GENERAL REMARKS

5. As a general remark, the Board notes that several criteria are phrased in too general terms, which may lead to confusion as to what needs to be audited by accredited certification bodies and how. In particular, the Board considers that certain criteria do not allow for repeated and consistent assessment by several accredited certification bodies. For example, in Section 6.1.2.b, it is not clear from the criterion how the certification body will verify that the applicant has satisfied the conditions for unambiguous consent. In this respect, the Board is of the opinion that the applicant must not only provide a statement that it respects the unambiguous nature of consent, but also provide material evidence of clear affirmative action from the data subjects (e.g. no pre-ticked boxes, written or oral statement, online proactive action from the data subject etc.) as well as proof of implementation of a procedure guaranteeing that consent is implemented as decided (e.g. interviews with data subjects, result of test panels carried out by the controller, etc.). The Board therefore recommends ensuring that each certification criterion is designed in such a way as to enable reproducible assessment by several certification bodies in a consistent manner.

This applies, inter alia, to the criteria listed below:

- In Section 5.3.2 (‘Data Protection Officer (DPO’)), the criteria on how to demonstrate that the DPO has expert knowledge of data protection and practice (Section 5.3.2.1.b), is consulted in the timely manner (Section 5.3.2.2.a), has active support from the Board (Section 5.3.2.2.b), or that the internal organization is aware of the existence of the DPO (5.3.2.2.d);
- In Section 6.1.2 (‘lawfulness’), the criteria in relation to the lawfulness of the processing, such as how the organization can demonstrate that the conditions for consent are met in practice (Section 6.1.2.b) or the processing pursues a legitimate interest in respect of the data subjects’ rights and freedoms (Section 6.1.2.g);
- In Section 6.2.3 (‘data minimisation’), the different possible processing scenarios envisaged by the organization should be provided;

6. The Board recalls that, in accordance with Article 43(6) GDPR, the Brand Compliance draft certification criteria must be made public by the supervisory authority in an easily accessible form. Therefore, the Board encourages that the copyright statement in this document be amended to clarify that the document will be made public by the supervisory authority in accordance with Article 43(6) GDPR.
7. Although the introductory part of the draft certification criteria specifies that Brand Compliance is a national certification mechanism referred to in the first sentence of Article 42(5) GDPR, the Board is of the view that the national scope of the criteria is not entirely clear in the criteria. In particular, the Board notes that the draft certification criteria includes multiple references to Member States “law” or “additional requirements”, for instance in Sections 5, 6, 7 and 8 and to the impact of the processing operations on data subjects in more than one Member State, for instance in sections 6.1.2.c and 8.2.1 of the scheme. According to the Board, this can lead to confusion as to the scope of the certification criteria. Consequently, the Board recommends clarifying the scope of Brand Compliance as a national certification scheme⁴.
8. The Board notes that the introduction refers to the obligation for the organisation to meet all the criteria contained in the Brand Compliance certification criteria “*unless [it] can demonstrate that the exclusions have no impact on the organisations ability to comply with the GDPR and this Standard*”. In this respect, the Board reiterates that none of the criteria set out in the certification scheme should simply be disregarded by the applicant, even if it claims to demonstrate its ability to comply with the GDPR in an alternative way. Although in some instances the applicability of certain criteria could be assessed by the applicant due to, for example, the scope of the ToE or the applicability of specific requirements under the GDPR (such as the appointment of a DPO), an assessment of these criteria should be carried out by the applicant and reviewed by the certification body. Therefore, the Board recommends to remove this sentence from the draft certification criteria.
9. The Board notes that the terminology used to name the certification criteria can be misleading as the title refers to “certification standard” and there is no reference to the word “criteria” as referred to in Articles 42(5) and 64(1)(c) of the GDPR. Therefore, the Board encourages to replace the term “standard” by “criteria” throughout the document.
10. The Board would welcome clarifications as to the meaning of some of the terms in Section 3.1 (‘Terminology’) by referring, where applicable, to the corresponding definition set out in Article 4 GDPR. For example, instead of explaining that “the term has the meaning as set out in the GDPR” the Board encourages to refer directly to the definitions in Article 4(7) for “controller”, Article 4(8) for “processor”, Article 4(11) for “consent”, Article 4(12) for “personal data breach”.
11. In addition, the Board notes the definition of “requirement” in Section 3.1 (‘Terminology’) as “*rule or legal obligation, agreement, need or legitimate expectation regarding the target of evaluation*”. However, the Board is of the opinion that it is unclear whether the use of the term “requirement” in Sections 4.2, 5.2.1, and “internal and external requirement” in Sections 3.1, 7.2.e, 7.2.f and 9.2.1.b, refers to technical and organisational measures (TOM), or additional data protection objectives. Therefore, the Board encourages clarifying the definition and the use of the term “requirement” throughout the draft certification criteria.

⁴ See Articles 42(4), 55 and 56 GDPR.

12. For the sake of consistency, the Board also recommends to adjust terminology used in the requirements to the one in the GDPR. This applies, in particular, to the following terms:
- In Section 6.1.2.b, point c), of the certification criteria the terms “can be freely given” should be replaced by “is freely given”.
 - In Section 6.1.3.b, the certification criteria refers to “the intake” and to “scope” of personal data while the GDPR refers to the “collection of personal data”;
 - In Section 6.1.4.c, the terms “further processing” and “not further processed” should be used instead of respectively “repeated use of personal data” or “frozen”;
 - In Section 8.6.g, the term “consent” should be replaced by “authorisation” in accordance with Article 28(2) GDPR;
 - In Section 8.4.8.b and 8.4.8.c., the term “[...] fully automated individual decision making” should be replaced by “[...] decision based solely on automated processing” instead in accordance with Article 22(1) GDPR.
 - Point 8.4 refers to the “right to restrict processing” instead of “right to restriction of processing”.
13. The numbering of the sections or some redirections to other sections of the certification criteria is sometimes inaccurate (e.g. note 2 under Section 6.1.2.d, Section 6.1.5, Section 6.4, Section 6.5, Section 7.4.a,). The Board therefore recommends to rectify the numbering of these sections accordingly.

2.2 SCOPE OF THE CERTIFICATION MECHANISM AND TARGET OF EVALUATION (TOE)

14. The Board notes that Section 4 contains criteria on how to define the ToE. In particular, Section 4.2.a sets out criteria for the organisation to determine and document the applicability of the GDPR, for which “*exclusion of implementation criteria shall be justified*”. In this regard, the Board recalls that the application or not of a specific criterion remains a decision from the certification body, not the applicant. Consequently, the Board recommends that this sentence be deleted from the draft certification criteria.
15. The Board notes that the certification criteria do not clearly indicate whether sub-processors can be certified under the scheme. In particular, the certification criteria do not entail specific criteria dedicated to sub-processors. In cases where the applicant to the scheme is a sub-processor, the Board considers that Section 8.6 would not be applicable. For example, in a sub-processing relationship, a sub-processor applying for certification would be conducting processing activities instructed by a processor and it would not necessarily be able to demonstrate that the instructions received originate from the controller as suggested under Section 8.6. Similarly, a sub-processor should have a dedicated obligation to inform the processor which is distinct to the obligation of information of Section 8.6.c. Moreover, in case of a data breach, Section 8.8.4 would not be applicable and there should be specific criteria adapted to the certification of sub-processors where the processor shall be notified by the sub-processor. In case sub-processors are eligible to certification, the Board recommends that specific criteria are developed to take into account the specificities of sub-processing. Alternatively, to make clear that sub-processors are outside the scope of this scheme the Board recommends to expressly indicate in the introduction that sub-processors cannot be certified under the Brand Compliance certification scheme.

16. The certification criteria are part of a general certification scheme applicable in the Netherlands, as referred to in Article 42(5) GDPR, and it therefore does not focus on a specific sector or type of processing activities. According to the information provided, the targeted audience consists of organisations "*in their role as controllers or processors, regardless of their type, size or the processing carried out in the framework of the products and services they provide*". The Board considers that the scope could be further specified by referring to "controllers, processors, joint controllers [and, if applicable, sub-processors]⁵" as well as the "type of product and services" provided by them and recommends to amend the introduction accordingly.
17. The Boards notes that Section 4 does not contain specific criteria regarding the identification of all data processing activities that would fall within the scope of the certification when defining the ToE. The Board highlights the fact that the description of the ToE should also include details on the role of the actors involved in the processing activities (e.g. data controller, data processor, joint-controller), as well as information on potential data transfers outside of the EU/EEA. The Board understands that some of these criteria have been developed under Section 4.2 and 4.3. However, the Board recommends to clarify that these criteria are to be assessed at an early stage when defining the ToE under Section 4.1.
18. Under Section 4.3, the certification criteria suggest that the duty to determine the scope of the certification lies on the applicant. Similarly, under Section 4.3.c the criteria suggest that it is the task of the applicant's management to approve the ToE and the scope of the certification. The Board highlights that the role of the applicant consists of precisely describing the intended scope of the certification and the ToE in its application for certification so they can be evaluated by a certification body. However, the applicant is not in charge of validating the scope of the criteria. The role of the applicant is limited to describing and proposing the scope of the certification mechanism and the ToE, whereas the certification body is to decide whether they are suitable for certification. The Board recommends to clarify that the decision on the determination of the scope of the certification and the ToE lies on the certification body after being suggested and described by the applicant.
19. In Section 5.3.2.1.d, the Board encourages to clarify that the organisation shall register the DPO with the Dutch Supervisory Authority given the national scope of the certification criteria.

2.3 LAWFULNESS OF PROCESSING

20. Under Section 6.1.2 ('Lawfulness'), the Board notes that the organisation shall "*determine that processing is allowed because at least one of the following conditions [for lawfulness] have been met*". In this regard, the Board considers that it should be made clear in the draft certification criteria that only one legal basis needs to be chosen and complied with from those listed in Article 6 GDPR. In addition, the Board is of the opinion that the certification criteria should include the requirement to demonstrate the applicability of the legal basis and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing. The Board therefore recommends to amend Section 6.1.2 accordingly.

⁵ See Recommendation under paragraph 15 of this Opinion.

21. The Board notes that some of the criteria in relation to consent are duplicated in Sections 6.1.2.b and 8.3.1.1.b. For the sake of clarity, the Board encourages to make clear links between the criteria instead of duplicating them. In addition, in Section 6.1.2. b ('Consent'), the Board recommends to add requirement with regard to children's consent in this section (for instance by referring to Section 8.3.1.1 in Section 6.1.2.c) as the conditions applicable to child's consent in relation to information society services is also one of the conditions to ensure lawfulness of the processing.
22. The Board notes that Section 6.1.2.c ('performance of the contact') includes the requirement for the processing "*to be related to the achievement of the main purpose of the contract, and not to any related interests of the organisation*". The Board encourages to clarify this sentence by stating that the processing should not go beyond the purpose that is integral part of the performance of the contract.
23. With regard to Section 6.1.2.h referring to Article 9 and 10 GDPR, the Board recommends to refer expressly to the conditions set out in these articles under which the prohibition does not apply.

2.4 PRINCIPLES OF ARTICLE 5

24. With regard to Section 6.1 ('Principles relating to the processing activities'), the Board notes that the use of the terms "principles of the GDPR" may be confusing and encourages to refer more specifically to the "principles in article 5 GDPR" .
25. In addition, the Board notes that point 6.1.a ("Policy regarding the principles") provides that the DPO must be consulted on the correct application of the principles in the case of new processing operations and substantial changes to existing processing operations. However, the Board observes that consultation of the DPO should not be limited to these cases. In the Board's opinion, the DPO, where appropriate, should also be consulted to assess the adequacy of the policy established on the application of these principles in accordance with Section 5.2.1.a. The Board encourages to clarify the role of the DPO in relation to these principles accordingly.
26. The Board notes that under Section 6.1.1 of the certification criteria, "*further processing for archiving in the general interest, for scientific or historic research, or statistical purposes is not considered to be incompatible with the original purposes*". The Board recommends to clarify that further processing for archiving in the public interest, scientific or historical research, or statistical purposes is not *per se* considered contrary to the original purpose (singular), provided that an assessment of the purpose compatibility is duly documented especially with regard to the existence of appropriate safeguards for the rights and freedoms of the data subject⁶. In particular, the Board is of the opinion that the appropriate safeguards for the rights and freedoms of data subjects in place for each processing operation carried out for archiving purposes in the public interest, for scientific or historical research or for statistical purposes should also be documented by the organisation and assessed as part of the compatibility test referred to in Section 6.1.1.c, point 3 (i), (ii) and (iii). Accordingly, the Board recommends adding a specific criterion in this respect in Section 6.1.1c, point 3 (i), (ii) and (iii).
27. In Section 6.1.1.d ('Necessity, proportionality and subsidiarity'), the Board encourages to clarify the requirements in this section, in particular their link with the principles under Article

⁶ See Recital 156 and Article 89(1) of the GDPR.

5 GDPR, as well as their interaction with the criteria related to the identification of a legal basis.

28. With regard to Section 6.1.1.1 ('Transfer of personal data to a third party'), the Board encourages that, in order to avoid any confusion with the notion of international transfer of personal data under Chapter V, the term "data transfer" be replaced by "data sharing" or "data transmission".
29. In Section 6.4.1 on "Data minimisation" the Board recommends to clarify, in accordance with Recital 39, that data minimisation principle requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. As regards Section 6.1.4.b ('Accuracy with repeated use'), the Board recommends to clarify the requirement "longer period of time" in order to allow the applicant to make an objective assessment of its compliance with this criteria.
30. In Section 6.1.5. ('Storage limitation'), the Board recommends to include the obligation for the organisation to ensure deletion by processors to whom data has been shared or transmitted, in accordance with Article 28(3)(g) GDPR. In addition, the Board recommends to remove reference in Section 6.1.5.a that "*the retention period [...] may be indefinite*" considering that personal data retention period should be determined in all cases. As regards Section 6.1.5 c ('Anonymisation'), the Board encourages the scheme owner to also include a reference to the cases in which anonymisation is carried out for the purposes of statistical or research purposes as per Article 89(1) GDPR. Finally, the Board notes that another use case leading to the deletion of data might be where the SA orders the erasure of personal data under Article 58(2)(g) GDPR and encourages to include this in the criteria.

2.5. GENERAL OBLIGATIONS FOR CONTROLLERS AND PROCESSORS

31. The Board notes that Section 6.2.a ('Assessing the processing instructions') may be subject to misinterpretation, as the sentence "*the organisation shall, where possible given the nature of the processing operation, establish, document and implement a process [...]*" could be understood as it is at the discretion of the processor to act in such a way. Therefore, the Board recommends to delete "where possible".
32. Regarding Section 6.5.1 ('Joint controllers') the Board notes that a data controller can submit to the Brand Compliance certification process a ToE which is subject to joint-controllership. In case the ToE is subject to joint-controllership, the Board wishes to underline that the accredited certification body will have to carefully conduct the application process to ensure that the ToE is meaningful and that the applicant is fully responsible for the compliance of the ToE with all obligations under the GDPR that the certification mechanism aims at demonstrating. As a consequence, the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the obligations under the GDPR might – depending on the context of the processing activities of the ToE - prevent the applicant to fulfil the criteria of certification. In this regard, while Section 6.4.1.c ('Evaluating the arrangements') notes that in such situations all controllers "*can only be certified as a whole in order to be meaningful to the target group*". Likewise, Note 3 under Section 4.3.a states that "*Processing operations for which several parties are joint controllers [...] the ToE must cover the processing operations of the joint controllers*", it remains unclear what this means for the certification process as such.

Therefore, when defining the ToE, the Board recommends to define the requirements to be met regarding the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the Brand Compliance certification criteria. Moreover, the Board recommends to include in Section 6.4.1.b ('Embedding the arrangements') criteria that implement the provisions of Article 26 (3) GDPR.

33. Regarding Section 8.8.4 ('Notification to the controller') the Board encourages to rephrase the sentence "*If and to the extent that it is not possible to provide the information at ones [once], it may be provided in stages without undue delay*" to make it clear that still all necessary information must be given, albeit at a later stage.
34. In Section 7.2.b ('Risk management procedure') the Board encourages to add references to Section 7.3 ('DPIA and prior consultation') to cover also the cases where the risks analysis and evaluation conclude that the processing would still result in a high residual risk. In addition, with regards to the last sentence of Section 7.2.b, the Board recommends to clarify that the procedure shall ensure that risk analyses, risk treatment plans and residual risks are clearly approved by the appropriate management.
35. While Section 8.7 ('International transfer of personal data (where applicable)') includes a comprehensive list of transfer tools available for third country transfers, the procedural aspect of that section is missing. The Board therefore recommends to add provisions on how to specifically meet the objective that the applicant demonstrably ensures GDPR compliance in that respect.
36. The Board notes that in Section 8.7.c ('Consulting the supervisory authority concerned') the reference to EDPB Recommendation 2/2020 is quite general and thus encourages to clarify the conditions in which a prior authorisation from the relevant supervisory authority is needed.

2.6 RIGHTS OF DATA SUBJECTS

37. Section 8.2.2 ('Providing information to the data subject') refers to the exemptions of the information obligation in Article 14 (5)(b) GDPR. However, the Board notes that it is missing a reference to the fact that where providing information is impossible or would involve a disproportionate effort, the controller must, in such cases, take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available. Therefore, the Board recommends to include this reference in order to align Section 8.2.2 with Article 14 (5)(b) GDPR. Furthermore, the Board recommends to clearly differentiate between the exemptions of the information obligation stipulated in Article 13(4) and Article 14 (5)(b) GDPR.
38. Section 8.2.2.b ('Preparing information to the data subjects') refers to the fact that "*the information provided to the data subject shall [...] be demonstrably agreed with (the representatives of) the data subjects*". However, the Board notes that the GDPR does not require a data subject "to agree" to information provided in line with Article 13 or Article 14 GDPR. Therefore, the Board recommends to use a different wording in Section 8.2.2.b in order to avoid misunderstandings.

39. The Board notes that Section 8.4.1.d ('Securing personal data (where applicable)') seems to apply only where personal data is stored "*for a short period of time*". However, in the view of the Board, a controller must always ensure compliance with the rights stipulated in Chapter III of the GDPR and, for example, not purposefully delete personal data when receiving an access request. Therefore, the Board recommends to delete the requirement "*for a short period of time*".
40. Regarding the handling of the rights of data subjects, Section 8.4.1.e ('Handling of the rights of the data subjects') refers to "[...] without undue delay and in no case later than 30 days" as timeline. In this regard, the Board recommends to refer instead to "[...] within one month of receipt of the request", as stipulated in Article 12 (3) GDPR.
41. Section 8.4.2.b ('Providing a copy') foresees that the organisation "*provides [...] the data subject, upon lawful and executable request, with a copy in a permanent form of his or her personal data that was processed by the organization*". In order to avoid misunderstandings and different interpretations of this provision the Board recommends to refer instead to the need for the organisation to "[...] provide a copy of the personal data undergoing processing", as stipulated in Article 15 (3) GDPR.
42. Regarding the right to erasure, Section 8.4.4.a states that "*The organisation shall determine and document whether and under what conditions the right of erasure applies to the processing activities*". The Board encourages to include a reference to Article 17 (3) GDPR to also cover and appropriately document situations where the right to erasure does not apply.
43. The Board notes that Section 8.4.6 ('The right to data portability (where applicable)') refers to the obligation for the organisation to, "[...] where technically feasible, transmit such data directly to the intended recipient" is used at the beginning of this section. In this respect, the Board recommends to use the wording "[...] to another controller without hindrance", as stipulated in Article 20 (1) GDPR, to clarify that "another controller" refers to the one indicated by the data subject, and to indicate that the personal data covered by the right to data portability also includes data generated by the observation of the data subject's activity.
44. Section 8.4.7 ('The right to object'), refers to the processing for "[...] scientific or historical purposes". In this respect however, the Board recommends to use the wording "[...] scientific or historical research purposes or statistical purposes", as stipulated in Article 21 (6) GDPR.
45. Regarding the title of Section 8.4.8 ('The right regarding automated decision-making'), the Board recommends to change it to "*the right regarding automated individual decision-making, including profiling*", in line with the title of Article 22 GDPR. In addition, the Board notes that the part on "objective" under the same section refers to the need for the organisation to "*ensure that automated individual decision making, including profiling, is carried out carefully*". As it may not be possible to assess its implementation in practice, the Board recommends deleting the word "carefully" from this paragraph.
46. According to Section 8.4.8.f ('Bias check'), the "[...] organisation shall demonstrably perform systematic analyses, at least annually, to determine the accuracy of the decision-making process and the absence of bias (distortion of results), and shall adjust the process as necessary." In the view of the Board, it is not entirely clear if Section 8.4.8.f considers the "absence of bias" as an aspect of data accuracy. In any case, in order to avoid misunderstandings, the Board encourages to include a reference to Recital 71 GDPR in Section 8.4.8.f, as data accuracy in the context of profiling and of Article 22 GDPR is addressed there.

47. Section 8.4.10 foresees that where “[...] the organisation refuses to comply with a request, it shall provide evidence that the request is manifestly unfounded or excessive”. In contradiction to Article 12(5) GDPR, Section 8.4.10 could be misunderstood that in cases where the controller charges a reasonable fee for handling a data subject request, there is no such demonstration obligation. Therefore, the Board recommends to make clear that the burden of demonstrating the manifestly unfounded or excessive character of the request applies to both scenarios mentioned in Article 12 (5) (a) and (b) GDPR.
48. Regarding Section 8.4.11, the Board recommends to clarify whether the “complaints procedure” refer to dispute resolution processes or to formal complaints pursuant to Article 77 (1) GDPR.

2.7 RISKS FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS

49. Regarding Section 7.3a, the Board recommends to include a reference to the lists pursuant to Article 35 (4) and (5) GDPR, as published by the NL SA.
50. The last sentence of Section 7.3.2 states “[...] or if the organisation develops processing operations under its own direction, comply with the requirements of Section 7.3 itself.” The EDPB notes that in cases where an alleged processor develops processing operations under its own direction, the processor would not be a processor but a controller and then Section 7.3.2 would not be applicable at all. Therefore, the Board recommends to delete the last sentence of Section 7.3.2.

2.8 TECHNICAL AND ORGANISATIONAL MEASURES GUARANTEEING PROTECTION

51. The Board considers that it is not clear to what extent the term “controls” referred to in Section 7.2 (‘Risk management’) differs from the notion of “technical and organisational measures”. The Board encourages to clarify this point accordingly.
55. The board notes that Section 7.4 (‘Data protection by design and by default’) of the certification criteria addresses the obligations related to data protection by design and by default pursuant to article 25 GDPR and encourages to include a reference to the criteria on processors and sub-processors already in Section 8.2.5, by taking them into account when contracting with these parties and when regularly reviewing and assessing processors’ operations.
56. Similarly, the Board encourages to emphasise that processors should seek to facilitate data protection by design and by default in order to support the controllers’ ability to comply with Article 25 obligations.
57. Finally, Section 7.5.1 (‘Competences’) refers to the need for the organisation to, “*where appropriate, take steps to acquire the necessary competence and evaluate the effectiveness of the steps taken*”. In the Board’s view, the need to ensure that the persons carrying out the data processing activities have the required competences should always be assessed and ensured. The Board therefore encourages to amend this criteria accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

By way of conclusion, the EDPB considers that:

regarding the “*general remarks*” the Board recommends that the NL SA

1. ensures throughout the certification scheme, that each certification criterion is designed in such a way as to enable reproducible assessment by several certification bodies in a consistent manner;
2. clarifies throughout the certification scheme, that the scope is a national certification;
3. deletes in the introductory part reference to “*unless [it] “can demonstrate that the exclusions have no impact on the organisations ability to comply with the GDPR and this Standard”*”;
4. adjusts throughout the certification scheme the terminology used in the requirements to the one in the GDPR;
5. rectifies throughout the certification scheme the numbering of sections or some redirections to other sections that are inaccurate.

regarding the “*scope of the certification mechanism and target of evaluation (ToE)*”, the Board recommends that the NL SA

1. removes in Section 4.2.a reference according to which “*exclusion of implementation criteria shall be justified*”;
2. includes in the certification scheme specific criteria to take into account the specificities of sub-processing or, in the alternative, indicates, in the introductory part, that sub-processors cannot be certified under the certification scheme;
3. amends the introduction to further specify the scope by referring to “*controllers, processors, joint controllers [and, if applicable, sub-processors]*” as well as the “*type of product and services*” provided by them;
4. clarifies in Section 4.1 that the assessment of all data processing activities that would fall within the scope of the certification are to be defined at the early stage of the definition of the ToE;
5. clarifies in Section 4.3 that the decision on the determination of the scope of the certification and ToE lies on the certification body after being suggested and described by the applicant.

regarding the “*lawfulness of the processing*” the Board recommends that the NL SA

1. amends Section 6.1.2 to make clear that only one legal basis needs to be chosen and complied with from those listed in Article 6 GDPR.
2. amends Section 6.1.2 to include the requirement to demonstrate the applicability of the legal basis and its appropriateness, where relevant, considering the processing activities, depending on the nature, context, scope and purposes of the processing;
3. adds a requirement in relation to children’s consent in Section 6.1.2.b;
4. refers expressly to the conditions set out in Article 9 and 10 GDPR in Section 6.1.2.h.

regarding the “*principles of Article 5*” the Board recommends that the NL SA

1. clarifies in Section 6.1.1 that further processing for archiving in the public interest, scientific or historical research, or statistical purposes is not *per se* considered contrary to the original purpose (singular) provided that an assessment of the purpose compatibility is duly documented especially with regard to the existence of appropriate safeguards for the rights and freedoms of the data subject

2. adds in Section 6.1.1.c, point 3 (i), (ii) and (iii) a specific criterion according to which the appropriate safeguards for the rights and freedoms of data subjects in place for each processing operation carried out for archiving purposes in the public interest, for scientific or historical research or for statistical purposes should also be documented by the organisation and assessed as part of the compatibility test referred to in Section 6.1.1.c point 3 (i), (ii) and (iii);
3. clarifies in Section 6.4.1 that data minimisation principle requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum;
4. clarifies in Section 6.1.4.b the requirement of « *longer period of time* » in order to allow for objective assessment by the applicant of its compliance with this criteria;
5. includes in Section 6.1.5 the obligation for the organisation to ensure deletion by processors to whom data has been shared or transmitted in accordance with Article 28(3)(g) GDPR;
6. deletes in Section 6.1.5 the reference that “*the retention period [...] may be indefinite*”.

regarding the “*general obligations for controllers and processors*” the Board recommends that the NL SA

1. deletes “where possible” in Section 6.2.a;
2. defines the requirements to be met regarding the arrangement concluded between the applicant and the other joint controllers involved in the ToE with regards to their respective responsibilities for compliance with the Brand Compliance certification criteria;
3. includes in Section 6.4.1.b criteria implementing the provisions of Article 26 (3) GDPR;
4. clarify in Section 7.2.b that the procedure shall ensure that risk analyses, risk treatment plans and residual risks are clearly approved by the appropriate management
5. includes in Section 8.7 provisions on how to specifically meet the objective that the applicant demonstrably ensures GDPR compliance in respect of data transfers;

regarding the “*rights of data subjects*” the Board recommends that the NL SA

1. includes in Section 8.2.2 a reference to the fact that where providing information is impossible or would involve a disproportionate effort, the controller must, in such cases, take appropriate measures to protect the data subject’s rights and freedoms and legitimate interests, including making the information publicly available;
2. makes a clear distinction in Section 8.2.2 between the exemptions of the information obligation stipulated in Article 13(4) and Article 14 (5)(b) GDPR;
3. amend Section 8.2.2.b to make clear that the GDPR does not require a data subject “to agree” to information provided in line with Article 13 or Article 14 GDPR;
4. deletes in Section 8.4.1.d the reference to “*for a short period of time*”;
5. refers in Section 8.4.1.e to “[...] *within one month of receipt of the request*”, as stipulated in Article 12 (3) GDPR;
6. refers in Section 8.4.2.b to the need for the organisation to “*[...] provide a copy of the personal data undergoing processing*”, as stipulated in Article 15 (3) GDPR;
7. uses in Section 8.4.6 the wording “[...] *to another controller without hindrance*”, as stipulated in Article 20 (1) GDPR to clarify that “another controller” refers to the one indicated by the data subject, and to indicate that the personal data covered by the right to data portability also includes data generated by the observation of the data subject’s activity;
8. uses in Section 8.4.7 the wording “[...] *scientific or historical research purposes or statistical purposes*”, as stipulated in Article 21 (6) GDPR;
9. amends the title of Section 8.4.8 to refer to “*the right regarding automated individual decision-making, including profiling*”, in line with the title of Article 22 GDPR;

10. deletes in Section 8.4.8 reference to the term “carefully”;
11. makes clear in Section 8.4.10 that the burden of demonstrating the manifestly unfounded or excessive character of the request applies for both scenarios mentioned in Article 12 (5) (a) and (b) GDPR;
12. clarifies in Section 8.4.11 whether the “complaints procedure” refer to dispute resolution processes or to formal complaints pursuant to Article 77 (1) GDPR.

regarding the *“risks for the rights and freedoms of natural persons”* the Board recommends that the NL SA

1. includes in Section 7.3a a reference to the lists pursuant to Article 35 (4) and (5) GDPR, as published by the Supervisory Authority of the Netherlands;
2. deletes the last sentence of Section 7.3.2.

Finally, in line with the Guidelines the EDPB also recalls that, in case of amendments of the Brand Compliance certification criteria involving substantial changes⁷, the NL SA will have to submit the modified version to the EDPB in accordance with Articles 42(5) and 43(2)(b) of the GDPR.

4 FINAL REMARKS

This Opinion is addressed to the NL SA and will be made public pursuant to Article 64(5)(b) of the GDPR.

According to Article 64(7) and (8) of the GDPR, the NL SA shall communicate its response to this Opinion to the Chair by electronic means within two weeks after receiving the Opinion, whether it will amend or maintain its draft decision. Within the same period, it shall provide the amended draft decision or where it does not intend to follow the Opinion of the Board, it shall provide the relevant grounds for which it does not intend to follow this Opinion, in whole or in part.

Pursuant to Article 70(1)(y) GDPR, the NL SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

The EDPB recalls that, pursuant to Article 43(6) of the GDPR, the NL SA shall make public the certification criteria in an easily accessible form, and transmit them to the Board for inclusion in the public register of certification mechanisms and data protection seals, as per Article 42(8) of the GDPR.

For the European Data Protection Board
The Chair

(Anu Talus)

⁷ See section 9 of the Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation providing “Guidance on certification criteria assessment” for which the public consultation period expired on 26 May 2021.

Opinion of the Board (Art. 64)



Opinion 18/2023 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of the Collibra Group

Adopted on 7 November 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Collibra NV and its entities (hereinafter the “**Collibra Group**”) was reviewed by the Belgian SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Collibra Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 18 September 2023. The decision on the completeness of the file was taken on 4 October 2023.

2 ASSESSMENT

3. The draft BCR-P of the Collibra Group covers all intra-Group transfers and processing of personal data by Collibra group entities legally bound by the BCR-P including when they act as processors on behalf of third party controllers outside of the group in the EEA⁷.
4. Concerned data subjects include Collibra Group’s members, end users and customers, and their customers and users⁸.
5. The draft BCR-P of the Collibra Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Collibra Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Collibra Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Collibra Group BCR-P, Section 1 of Part I.

⁸ Collibra Group BCR-P, Section 2 of Part I.

of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



**Opinion 19/2023 on the draft decision of the Dutch
Supervisory Authority regarding the Controller Binding
Corporate Rules of the American Express Global Business
Travel Group**

Adopted on 16 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of American Express Global Business Travel (GBT) and its subsidiaries (hereinafter the "**GBT Group**") was reviewed by the Dutch SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the GBT Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 11 October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the GBT Group covers the processing of personal data by GBT Group as well as intra-group transfers of personal data to third countries within GBT companies legally bound by the BCR⁹.
4. Concerned data subjects include customers and their travellers, meeting attendees, service providers, employees (including former), directors, individual consultants, contingent workers, retirees, job applicants as well as any data given to GBT by such persons relating to third parties¹⁰.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ See GBT Scope and Purpose (p.1) and Appendix 1 List of GBT companies and Appendix 2 Description of processing and data flows.

¹⁰ See GBT Scope and Purpose (p.1) and Appendix 2.

5. The draft BCR-C of the GBT Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the GBT Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-group Agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the GBT Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 20/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the Comcast Corporation Group

Adopted on 16 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Comcast Corporation and the group's entities (hereinafter the "**Comcast Corporation Group**") was reviewed by the Dutch SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Comcast Corporation Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 11 of October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the Comcast Corporation Group covers the processing of personal data by Comcast Corporation Group entities as well as intra-group transfers of personal data from the EEA to countries outside the EEA amongst the members of the Comcast Corporation Group entities listed and legally bound to comply with the BCR⁹.
4. Concerned data subjects include prospective, current and former employees, individual contractors, suppliers, business partners, customers and online users¹⁰.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Data Protection Policy – Part A, section 2 & Part F & Intra-group Agreement.

¹⁰ Data Protection Policy – Part A, Section 2 & Part D and E.

5. The draft BCR-C of the Comcast Corporation Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Comcast Corporation Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-group Agreement the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Comcast Corporation Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 21/2023 on the draft decision of the Belgian Supervisory Authority regarding the Processor Binding Corporate Rules of the UPS Group

Adopted on 16 November 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of UPS Europe SRL and the group's affiliates (hereinafter the "**UPS Group**") was reviewed by the Belgian SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the UPS Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 9 October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-P of the UPS Group covers all intra-Group transfers amongst UPS Group affiliates and all processing of personal data by members of the UPS Group affiliates legally bound by the BCR-P, when they act as processors on behalf of controllers outside of the Group⁷.
4. Concerned data subjects include the business partners and business customers⁸.
5. The draft BCR-P of the UPS Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the UPS Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-group agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the UPS Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Section 1.1 of the UPS BCR-P.

⁸ Sections 1.1 and 2.1 of the UPS BCR-P.

to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 22/2023 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules for employee data of the UPS Group

Adopted on 16 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C for employee data of UPS Europe SRL and the group's affiliates (hereinafter the "**UPS Group**") was reviewed by the Belgian SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C for employee data of the UPS Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 9 October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-C for employee data of the UPS Group covers intra-group transfers to third countries amongst the UPS Group affiliates and the processing of personal data by UPS group affiliates legally bound by this BCR⁹.
4. Concerned data subjects include current and former employees (including temporary workers, independent contractors and trainees), job applicants, current and former shareholders, current and

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Section 1.1 of the UPS BCR-C for employee data.

former executive or non-executive directors or members of the supervisory board, family members, dependents¹⁰.

5. The draft BCR-C for employee data of the UPS Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the UPS Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-group agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C for employee data of the UPS Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

¹⁰ Section 1.1 of the UPS BCR-C for employee data and Annex 1.

Opinion of the Board (Art. 64)



Opinion 23/2023 on the draft decision of the Belgian Supervisory Authority regarding the Controller Binding Corporate Rules for customer data of the UPS Group

Adopted on 16 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C for customer data of UPS Europe SRL and the group's affiliates (hereinafter the "**UPS Group**") was reviewed by the Belgian SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C for customer data of the UPS Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 9 October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-C for customer data of the UPS Group covers intra-group transfers to third countries amongst UPS Group affiliates and the processing of personal data by the UPS group affiliates legally bound by this BCR⁹.
4. Concerned data subjects include customers, suppliers, and business partners and other individuals¹⁰.
5. The draft BCR-C for customer data of the UPS Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Section 1.1 of the UPS BCR-C for customer data.

¹⁰ Section 1.1 of the UPS BCR-C for customer data.

UPS Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-group agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C for customer data of the UPS Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 24/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Nestlé Group

Adopted on 16 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the Nestlé SA Group and its affiliates, represented by Nestlé France SAS, (hereinafter the “**Nestlé Group**”) was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Nestlé Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 10 October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the Nestlé Group covers intra-group transfers of personal data to third countries amongst the members of the Nestlé Group affiliates legally bound to comply with the BCR, as well as to any onward international transfer within the Nestlé Group Affiliates, when Nestlé Group affiliates legally bound by the BCR act as controllers or as processors on behalf of another controller of the Group⁹.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Article 1 of the BCRs, as well as Appendix 1 providing a list of the defined terms.

4. Concerned data subjects include Nestlé Personnel, along with their family members and other beneficiaries, job applicants, consumers, website visitors, and those who visit Nestlé's facilities, as well as the personnel of corporate customers and vendors, third parties such as occasional journalists interacting with Nestlé, and participants in product development studies and clinical trials¹⁰.
5. The draft BCR-C of the Nestlé Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Nestlé Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Nestlé Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

¹⁰ Appendix 2 of the BCRs.

Opinion of the Board (Art. 64)



Opinion 25/2023 on the draft decision of the Dutch Supervisory Authority regarding the Controller Binding Corporate Rules of the SHV Holding N.V. Group

Adopted on 16 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of SHV Holdings N.V. and its subsidiaries (hereinafter the “SHV Group”) was reviewed by the Dutch SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the SHV Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on the 11th of October 2023. The decision on the completeness of the file was taken on 23 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the SHV Group covers transfers the processing of personal data by SHV Group as well as intra-group transfers of personal data to third countries within the SHV Group legally bound by the BCR⁹.
4. Concerned data subjects include customers, suppliers, employees and their dependents, business partners, and other individuals¹⁰.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Employee Code: Article 1.5. & Customer Code: Article 1.5. & Application Form: Section 4, Annex I.

¹⁰ Employee Code: Article 1.1. & Customer Code: Article 1.1 & Application Form 7.

5. The draft BCR-C of the SHV Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the SHV Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Intra-group Agreement*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the SHV Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 26/2023 on the draft decision of the Romanian Supervisory Authority regarding the Processor Binding Corporate Rules of the OSF Global Services Group

Adopted on 16 October 2023

Version 1.1	28 11 2023	Corrigendum of the Art. 64 Opinion title to state that it is Opinion 26/2023 and not Opinion 10/2023.
Version 1.0	20 11 2023	Adoption of the Art. 64 Opinion after written procedure: Opinion 10/2023 on the draft decision of the Romanian Supervisory Authority regarding the Processor Binding Corporate Rules of the OSF Global Services Group

Table of contents

1	SUMMARY OF THE FACTS.....	6
2	ASSESSMENT.....	6
3	CONCLUSIONS / RECOMMENDATIONS.....	6
4	FINAL REMARKS.....	7

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU .

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data i instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of **SC OSF Global Services SRL** and the group's entities (hereinafter the "**OSF Global Services Group**") was reviewed by the Romanian SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the OSF Global Services Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 9 August 2023. The decision on the completeness of the file was taken on 22 August 2023.

2 ASSESSMENT

3. The draft BCR-P of the OSF Global Services Group covers the processing of personal data by OSF Global Services Group entities as well as intra-group direct and indirect transfers of personal data from OSF Global Services entities acting as processors in the EEA to OSF Global Services entities acting as sub-processors outside the EEA⁷.
4. Concerned data subjects include prospective and current customers including their own clients, employees and representatives or other personnel having a contractual relationship with current customers or prospective customers.⁸
5. The draft BCR-P of the OSF Global Services Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the OSF Global Services Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS / RECOMMENDATIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the *Intra-Group Agreement*, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the OSF Global Services Group contains appropriate safeguards

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ OSF Binding Corporate Rules, p. 8, 3.2, "Geographical Scope".

⁸ OSF Binding Corporate Rules, p. 8, 3.1, "Material Scope".

to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 27/2023 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Tessi Group

Adopted on 28 November 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Tessi and its entities (hereinafter the “**Tessi Group**”), represented by Tessi SAS, was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Tessi Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 26 October 2023. The decision on the completeness of the file was taken on 31 October 2023.

2 ASSESSMENT

3. The draft BCR-P of the Tessi Group covers all processing operations involving the direct and indirect transfer of personal data carried out by Tessi Group entities established within the EEA, in their capacity as processor to Tessi Group entities established outside the EEA. They also cover transfers of personal data carried out by Tessi Group entities established outside the EEA, as data exporter, transferring personal data to Tessi Group entities also established outside the EEA as data importer insofar as the GDPR applies to such processing in accordance with the conditions provided for in Article 3.2 of the GDPR⁷.
4. Concerned data subjects include employees, interns, customers, business partners, suppliers, service providers and subcontractors of their customers⁸.
5. The draft BCR-P of the Tessi Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Tessi Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the intra-group agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Section III.1 of the BCRs.

⁸ Section III.2.1 and in appendix 11 of the BCRs.

as it is, since the draft BCR-P of the Tessi Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 28/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Servier Group

Adopted on 28 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the Servier Group and its affiliates, represented by Servier SAS, (hereinafter the "**Servier Group**") was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Servier Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 26 October 2023. The decision on the completeness of the file was taken on 31 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the Servier Group covers all processing of Personal Data carried out by SERVIER Companies⁹.
4. Concerned data subjects include Servier's employees, contractors, clients, customers, suppliers, service providers and other third parties as part of the Group's respective regular business activities¹⁰.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Article 4 of the BCRs. Appendix 2 includes a list of SERVIER Companies that are bound by the BCRs.

¹⁰ The complete list of data subjects categories are detailed in Appendix 3 of the BCRs.

5. The draft BCR-C of the Servier Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Servier Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the Intra-Group Agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Servier Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 29/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Sodexo Group

Adopted on 28 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of the Sodexo group and its entities (hereinafter the “**Sodexo Group**”), represented by Sodexo SA, was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Sodexo Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 26 October 2023. The decision on the completeness of the file was taken on 31 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the Sodexo Group covers the processing of Personal Data by Sodexo entities established within Europe legally bound by the BCRs when they act as controllers or as processors on behalf of another controller of the Group and to all subsequent processing of Personal Data from Sodexo entities outside Europe to any other Sodexo entities within the Group⁹.

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Section “What is the purpose and the scope of the Sodexo BCR?” of the General Introduction of the BCRs.

4. Concerned data subjects include Sodexo's current, past and prospective job applicants, employees, clients, consumers/beneficiaries, suppliers/vendors, contractors/subcontractors, or any third parties or by a third-party on behalf of Sodexo.¹⁰
5. The draft BCR-C of the Sodexo Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Sodexo Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the intragroup agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Sodexo Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

¹⁰ Section "What is the purpose and the scope of the Sodexo BCR?" of the General Introduction of the BCRs and appendix 8.

Opinion of the Board (Art. 64)



**Opinion 30/2023 on the draft decision of the French
Supervisory Authority regarding the Processor Binding
Corporate Rules of the Sodexo Group**

Adopted on 28 November 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of the Sodexo Group and its entities (hereinafter the “**Sodexo Group**”), represented by Sodexo SA, was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Sodexo Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 26 October 2023. The decision on the completeness of the file was taken on 31 October 2023.

2 ASSESSMENT

3. The draft BCR-P of the Sodexo Group covers all flows of Personal Data processed by Sodexo on behalf of a Controller for processing activities within the Group entities legally bound by BCR-P, whatever the origin of the Personal Data⁷.
4. Concerned data subjects include Sodexo’s current, past and prospective clients, consumers/beneficiaries, as well as such Processing on behalf of a Client⁸.
5. The draft BCR-P of the Sodexo Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Sodexo Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the intragroup agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Sodexo Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Section “What is the purpose and the scope of the Sodexo BCR?” of the General Introduction of the BCRs.

⁸ Section “What is the purpose and the scope of the Sodexo BCR?” of the General Introduction of the BCRs and appendix 7.

the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 31/2023 on the draft decision of the French Supervisory Authority regarding the Controller Binding Corporate Rules of the Thalès Group

Adopted on 28 November 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Thalès S.A. and its entities (hereinafter the "**Thalès Group**") was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Thalès Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 23 October 2023. The decision on the completeness of the file was taken on 31 October 2023.

2 ASSESSMENT

3. The draft BCR-C of the Thalès Group apply when a BCR member is acting as a data controller or as an internal data processor. They apply to transfers of personal data from BCR members within the EEA to BCR members located outside the EEA, as well as to their onward transfers to other BCR members outside the EEA⁹.
4. Concerned data subjects include (i) THALES' employees, including THALES' salaried employees, representatives and officers, as well as THALES' former employees; (ii) THALES' temporary workers and interns; (iii) THALES' job applicants; (iv) employees and contact points of THALES' clients and prospects;

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Articles 2.2 and 2.3 of the BCRs and appendices 8 and 9 of the BCRs

- (v) employees and contact points of THALES' partners, providers, suppliers and subcontractors; (vi) users of application and public data subjects; and (vii) employees, contact points and clients of internal clients (internal client means any THALES entity acting as data controller, for which another THALES entity processes personal data in the frame of a contract for the provision of services or products implying personal data processing)¹⁰.
5. The draft BCR-C of the Thalès Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Thalès Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the intragroup agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Thalès Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

¹⁰ article 2.2 of the BCRs and appendix 1 of the BCRs

Opinion of the Board (Art. 64)



Opinion 32/2023 on the draft decision of the French Supervisory Authority regarding the Processor Binding Corporate Rules of the Thalès Group

Adopted on 28 November 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT	5
3	CONCLUSIONS	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Thalès S.A. and its entities (hereinafter the “**Thalès Group**”) was reviewed by the French SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Thalès Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 23 October 2023. The decision on the completeness of the file was taken on 31 October 2023.

2 ASSESSMENT

3. The draft BCR-P of the Thalès Group apply when a BCR member is acting as a data processor. They apply to transfers of personal data from BCR members within the EEA to BCR members located outside the EEA, as well as to their onward transfers to other BCR members outside the EEA⁷.
4. Concerned data subjects include clients, clients’ employees; clients’ clients; employees of clients’ clients; providers and suppliers; employees of providers and suppliers⁸.
5. The draft BCR-P of the Thalès Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Thalès Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the intragroup agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Thalès Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Articles 2.2 and 2.3 of the BCRs and appendices 7 and 8 of the BCRs

⁸ Article 2.2 of the BCRs

to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 33/2023 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Controller Binding Corporate Rules of the Cerner Group

Adopted on 13 December 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS.....	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Cerner Health Services Deutschland GmbH and its participating group companies (hereinafter the “**Cerner Group**”) was reviewed by the Hesse Supervisory Authority (Germany) as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Cerner Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 24 October 2023. The decision on the completeness of the file was taken on 20 November 2023.

2 ASSESSMENT

3. The draft BCR-C of the Cerner Group covers any transfer or sharing of personal data within Cerner Group companies legally bound by the BCR, i. e. from a participating Cerner Group company established in the European Economic Area and acting as a controller or internal processor to a participating Cerner group company in a third country⁹.
4. Concerned data subjects include employees, prospective employees and applicants, customer workforce members, users of Cerner solutions and services, suppliers, business partners, prospective

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁹ Section 1 and Section 17 of the BCR-C Policy.

business partners and other data subjects affected in the course of Cerner business such as interested individuals, regulator contact data or third-party auditors¹⁰.

5. The draft BCR-C of the Cerner Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Cerner Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the BCR Implementation Agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Cerner Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

¹⁰ Section 18 of the BCR-C Policy.

Opinion of the Board (Art. 64)



Opinion 34/2023 on the draft decision of the Hesse Supervisory Authority (Germany) regarding the Processor Binding Corporate Rules of the Cerner Group

Adopted on 13 December 2023

Table of contents

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS.....	5
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the decision of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings is intended to provide guarantees that apply uniformly in all third countries and, consequently,

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party², endorsed by the EDPB.

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB³. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP257 rev.01 of the Article 29 Working Party, as endorsed by the EDPB, provides for the required elements for BCRs for processors (hereinafter “**BCR-P**”), including the Intra-Company Agreement where applicable, and the application form. The WP265 of the Article 29 Working Party⁴, as endorsed by the EDPB, provides for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP257 rev.01. Additionally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs’ national laws and with Regulation 1049/2001⁵, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP265.

⁵ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁶.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-P of Cerner Health Services Deutschland GmbH and its participating group companies (hereinafter the “**Cerner Group**”) was reviewed by the Hesse Supervisory Authority (Germany) as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-P of the Cerner Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 24 October 2023. The decision on the completeness of the file was taken on 20 November 2023.

2 ASSESSMENT

3. The draft BCR-P of the Cerner Group covers any transfer or sharing of personal data within Cerner Group companies legally bound by the BCR, i. e. from a participating Cerner Group company established in the European Economic Area (EEA) and acting as a processor or sub-processor on behalf of and under the instructions of a client established in the EEA to a participating Cerner Group company in a third country⁷.
4. Concerned data subjects include Cerner clients (including client patients) for which Cerner is acting as a processor.⁸
5. The draft BCR-P of the Cerner Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-P of the Cerner Group contains all the elements required under Article 47 GDPR and WP257 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

6. Taking into account the above and the commitments that the group members will undertake by signing the BCR Implementation Agreement, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-P of the Cerner Group contains appropriate safeguards to

⁶ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

⁷ Sections 1, 17 and 18 of the BCR-P Policy.

⁸ Section 17 of the BCR-P Policy.

ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.

7. Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP257 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

8. This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
9. According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
10. Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

Opinion of the Board (Art. 64)



Opinion 35/2023 on the draft decision of the Danish Supervisory Authority regarding the Controller Binding Corporate Rules of the Carlsberg Group

Adopted on 13 December 2023

TABLE OF CONTENTS

1	SUMMARY OF THE FACTS.....	5
2	ASSESSMENT.....	5
3	CONCLUSIONS.....	6
4	FINAL REMARKS.....	6

The European Data Protection Board

Having regard to Article 63, Article 64(1)(f) and Article 47 of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter “**GDPR**”),

Having regard to the European Economic Area (hereinafter “**EEA**”) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to the judgment of the Court of Justice of the European Union *Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*, C-311/18 of 16 July 2020,

Having regard to EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data of 18 June 2021,

Having regard to EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR) of 20 June 2023,

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) The main role of the European Data Protection Board (hereinafter the “**EDPB**”) is to ensure the consistent application of the GDPR throughout the EEA. To this effect, it follows from Article 64(1)(f) GDPR that the EDPB shall issue an opinion where a supervisory authority (hereinafter “**SA**”) aims to approve binding corporate rules (hereinafter “**BCRs**”) within the meaning of Article 47 GDPR.

(2) The EDPB welcomes and acknowledges the efforts the companies make to uphold the GDPR standards in a global environment. Building on the experience under Directive 95/46/EC, the EDPB affirms the important role of BCRs to frame international transfers and its commitment to support the companies in setting-up their BCRs. This opinion aims towards this objective and takes into account that the GDPR strengthened the level of protection, as reflected in the requirements of Article 47 GDPR, and conferred to the EDPB the task to issue an opinion on the competent SA’s draft decision aiming to approve BCRs. This task of the EDPB aims to ensure the consistent application of the GDPR, including by the SAs, controllers, and processors.

(3) Pursuant to Article 46(1) GDPR, in the absence of a decision pursuant to Article 45(3) GDPR, a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. A group of undertakings or group of enterprises engaged in a joint economic activity may provide such safeguards by the use of legally binding BCRs, which expressly confer enforceable rights on data subjects and fulfil a series of requirements (Article 46 GDPR). The implementation and adoption of BCRs by a group of undertakings

¹ References to “Member States” made throughout this opinion should be understood as references to “EEA Member States”.

is intended to provide guarantees that apply uniformly in all third countries and, consequently, independently of the level of protection guaranteed in each third country. The specific requirements listed in the GDPR are the minimum items BCRs shall specify (Article 47(2) GDPR). The BCRs are subject to approval from the competent SA (hereinafter “**the BCR Lead**”), in accordance with the consistency mechanism set out in Article 63 and Article 64(1)(f) GDPR, provided that the BCRs meet the conditions set out in Article 47 GDPR, together with the requirements set out in the relevant working documents of the Article 29 Working Party² endorsed by the EDPB or, as the case may be, in the EDPB Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR), adopted on 20 June 2023 (hereinafter “**the Recommendations**”).

(4) This opinion only covers the EDPB’s consideration that the BCRs submitted for the required opinion afford appropriate safeguards in that they meet all requirements of Article 47 GDPR and the relevant documents of the Article 29 Working Party or the EDPB, as the case may be. Accordingly, this opinion and the SAs’ review do not address elements and obligations of the GDPR mentioned in the BCRs at issue other than those related to Article 47 GDPR. This also applies to any supplementary measures that an exporter subject to the GDPR may be required to adopt, depending on the circumstances of the transfer, in order to ensure compliance with the commitments taken in the BCRs.

(5) The EDPB recalls that, in accordance with the judgment of the Court of Justice of the European Union C-311/18 , it is the responsibility of the data exporter subject to the GDPR, if needed with the help of the data importer, to assess whether the level of protection required by EU law is respected in the third country concerned, in order to determine if the guarantees provided by BCRs can be complied with in practice, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter subject to the GDPR, if needed with the help of the data importer, should assess whether they can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EU.

(6) The WP256 rev.01 of the Article 29 Working Party³ provided for the required elements for BCRs for controllers (hereinafter “**BCR-C**”), including the Intra-Company Agreement where applicable, and the application form. The WP264 of the Article 29 Working Party⁴, provided for recommendations to the applicants to help them demonstrate how to meet the requirements of Article 47 GDPR and WP256 rev.01. The EDPB notes that WP256 rev.01 and WP264 are now superseded by the Recommendations. However, in accordance with paragraph 13 of the Recommendations, the BCR-Cs that had already reached the stage of a “consolidated draft” in accordance with 2.4 of WP 263 rev.01⁵ at the time of the publication of the Recommendations (30 June 2023), could be assessed under the previous framework (i.e. WP256 rev.01 and WP264), subject to the EDPB adopting its opinion by the

² The Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

³ Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01. The document was endorsed by the EDPB on 25 May 2018.

⁴ Article 29 Working Party, Recommendations on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, adopted on 11 April 2018, WP264.

⁵ WP29 Working Document setting forth a co-operation procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP263 rev.01, adopted on 11 April 2018, endorsed by the EDPB.

end of 2023. This being the case of the present BCR-C, the assessment of compliance has been undertaken in accordance with WP256 rev.01. The EDPB underlines that the BCR-C will have to be brought in line with the Recommendations at its 2024 annual update⁶. Finally, the EDPB highlights that any documentation submitted may be subject to access to documents requests in accordance with the SAs' national laws and with Regulation 1049/2001⁷, applicable to the EDPB pursuant to Article 76(2) GDPR.

(7) Taking into account the specific characteristics of BCRs provided for by Article 47(1) and (2) GDPR, each application should be addressed individually and is without prejudice to the assessment of any other BCRs. The EDPB recalls that BCRs should be customised to take account of the structure of the group of companies that they apply to, the processing they undertake, and the policies and procedures that they have in place to protect personal data⁸.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks, taking into account the complexity of the subject matter.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in WP263 rev.01, the draft BCR-C of Carlsberg A/S and its corporate entities (hereinafter the “**Carlsberg Group**”) was reviewed by the Danish SA as the BCR Lead.
2. The BCR Lead has submitted its draft decision regarding the draft BCR-C of the Carlsberg Group, requesting an opinion of the EDPB pursuant to Article 64(1)(f) GDPR on 3 November 2023. The decision on the completeness of the file was taken on 13 November 2023.

2 ASSESSMENT

3. The draft BCR-C of the Carlsberg Group covers Carlsberg Entities that are legally bound by the BCR and which are processing personal data relating to data subjects, including all Carlsberg Entities established:
 - in the EEA or in a country with an adequate level of data protection as acknowledged by a decision of the European Commission; and

⁶ Recommendations 1/2022, paragraph 13.

⁷ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

⁸ This view was expressed by the Article 29 Working party in Working Document Setting up a framework for the structure of Binding Corporate Rules, adopted on 24 June 2008, WP154.

- outside the EEA or outside a country with an adequate level of data protection as acknowledged by a decision of the European Commission⁹.
- Concerned data subjects include employees, applicants, consultants, visitors, former employees, customers, suppliers and other business contacts¹⁰.
 - The draft BCR-C of the Carlsberg Group has been scrutinised according to the procedures set up by the EDPB. The SAs assembled within the EDPB have concluded that the draft BCR-C of the Carlsberg Group contains all the elements required under Article 47 GDPR and WP256 rev.01, in accordance with the draft decision of the BCR Lead submitted to the EDPB for an opinion. Therefore, the EDPB does not have any concerns that need to be addressed.

3 CONCLUSIONS

- Taking into account the above and the commitments that the group members will undertake by signing the Binding Corporate Rules Undertaking, the EDPB considers that the draft decision of the BCR Lead may be adopted as it is, since the draft BCR-C of the Carlsberg Group contains appropriate safeguards to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined when personal data is transferred to and processed by the group members based in third countries. The EDPB recalls that the approval of BCRs by the BCR Lead does not entail the approval of specific transfers of personal data to be carried out on the basis of the BCRs. Accordingly, the approval of BCRs may not be construed as the approval of transfers to third countries included in the BCRs for which an essentially equivalent level of protection to that guaranteed within the EU cannot be ensured.
- Finally, the EDPB also recalls the provisions contained within Article 47(2)(k) GDPR and WP256 rev.01 providing the conditions under which the applicant may modify or update the BCRs, including updates to the list of BCRs group members.

4 FINAL REMARKS

- This opinion is addressed to the BCR Lead and will be made public pursuant to Article 64(5)(b) GDPR.
- According to Article 64(7) and (8) GDPR, the BCR Lead shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.
- Pursuant to Article 70(1)(y) GDPR, the BCR Lead shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

For the European Data Protection Board

The Chair

(Anu Talus)

⁹ The BCR-C Policy clauses 3 and 4.

¹⁰ Carlsberg BCR - Appendix 7