

The Chair

[REDACTED]

Registered letter with A.R.

A.R. no.: 2C 127 845 4657 5

Investigation of the case:

Paris, on the 20th March 2019

Our Ref.: MLD/MJN/CLP191004

Referral no. 18019335

(To be quoted in all correspondence)

Dear Chief Executive,

I refer to the email exchange between my department and [REDACTED] your Data Protection Officer (hereinafter “DPO”), as part of the investigation into [REDACTED] [REDACTED] complaint, which was transferred to us by the supervisory authority of Berlin (Germany), pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] had lodged a complaint with this supervisory authority against [REDACTED] due to difficulties encountered in exercising his right to object to receiving marketing by email, on the one hand, and concerning the information given on the product order form on the [REDACTED] website, on the other hand.

Following the exchanges between the CNIL and [REDACTED] DPO, I inform you of the following decision.

This decision was taken in agreement with the supervisory authorities concerned by the marketing processing carried out by [REDACTED] in the different European Union countries.

Chiefly, as regards the exercise of the claimant’s right to object, I note that [REDACTED] request to unsubscribe was taken into account by your department on his first request dated 2 June 2018 through the unsubscribe link and that he has not received any emails from [REDACTED] since 8 June 2018.

In this respect, your DPO specifies that [REDACTED] continued to receive emails from 2 to 8 June 2018 due to the 72-hour delay that can occur between a request to object being made and the consideration this latter, this period being indicated in the email of acknowledgment of receipt that [REDACTED]. However, in this case, the request had been made on a Saturday and Monday 4 June was a bank holiday in France.

Furthermore, [REDACTED] states that the claimant sent his written requests to object dated 2, 3 and 5 June 2018 by using the “reply” feature on the marketing emails that he had received. These messages were sent by the address [REDACTED], which cannot be replied to. In this respect, your DPO specifies that this information will now clearly appear in the body of marketing emails.

Moreover, I note that the company [REDACTED] has set up a dedicated email address [REDACTED] to handle requests relating to personal data more efficiently since the entry into force of the GDPR. In particular, this email address appears on your website, including in its German version, in the “personal data” tab.

Lastly, your DPO specifies that “*when requests are actually made to [your] client services, these are quickly redirected to the Data Protection Officer, who processes these requests within one month, except for in complex cases*”.

Secondly, as regards the product order form on your website, I note that the indication of customers’ date of birth is no longer mandatory when purchasing online, including on the website’s German version. Indeed, the mandatory nature of a response is marked by an asterisk next to the field in question, which is not the case for dates of birth.

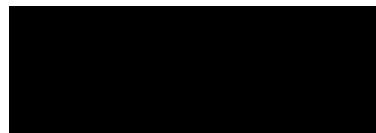
Furthermore, according to the checks performed by my department, I also note that the order form includes two boxes which clients must check in order to consent to receiving promotional offers from [REDACTED], in one case, and from its partners in the other.

These two boxes are also present in the German version of the order form on the [REDACTED] website.

All of these elements lead me to close this complaint against your organisation.

The CNIL reserves the right, in the event of any new claim, to use all powers afforded to it by the GDPR and by the Act of 6 January 1978 amended.

Yours faithfully,



Marie-Laure DENIS

Copy: [REDACTED], Data Protection Officer

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	22 March 2019
LSA:	FR
CSAs:	AT, BE, DE-Berlin, DE-Mecklenburg-Western Pomerania, DE-Bavaria (private sector), DE-Lower Saxony
Legal Reference:	Right to object (Article 21), Principles relating to processing of personal data (Article 5), Lawfulness of the processing (Article 6), Conditions for consent (Article 7)
Decision:	No violation
Key words:	Rights of data subjects, Right to object, Lawfulness of processing, e-Commerce, Marketing,

Summary of the Decision

Origin of the case

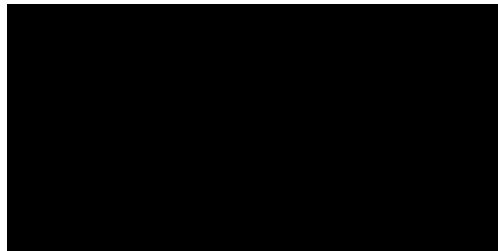
The data subject filed a complaint after facing difficulties in pursuing his right to object and in relation to the information required on the product order form.

Findings

The LSA found that the delay in complying with the right to object was due to the 72 hours required to process the relevant request, of which the data subject was informed. Besides, the request was submitted on a Saturday and Monday was a holiday. The data controller also took measures to clarify the e-mail address to which such requests can be submitted, and it also set up a dedicated email address to handle such requests more efficiently. In addition, the data controller no longer requires the date of birth to be provided for an order to be placed. Moreover, the consent to receive promotional offers from the controller and third parties must be explicitly given by checking the respective boxes when ordering a product.

Decision

The LSA did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by the controller. The data controller did not delay to comply with the request beyond what was reasonable and adjusted the information required to avoid collecting more data than necessary.

The President

Examination of the case:

20 MARS 2019

No./Ref. : MLD/XD/DAU/CM191143

Request no. 18019406**(to be recalled in any future correspondence)**

Dear Mr. Director-General,

This is further to the exchanges that took place between the CNIL's services and the marketing service of [REDACTED] in the framework of the examination of the complaint transmitted to us by the data protection authority of Rhineland-Palatinate (Germany) according to provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint was dealing with the information delivered to individuals visiting the website [REDACTED] as well as the conditions of processing of personal data for the purposes of direct marketing by your company.

Those exchanges are leading me, in agreement with other European data protection authorities concerned by your processing, **to proceed to the closure of this complaint.**

Indeed, I have noticed that the information delivered to individuals visiting the websites [REDACTED] has been updated, in accordance with Articles 13 and 14 of the GDPR on January 7th, 2019, by the publication on your different websites of a document entitled "*General Data Protection Regulation (GDPR)*".

Moreover, I have noted your commitment to pursue a consent campaign for the collection and the use of personal data for the purposes of direct marketing from data subjects, prior to sending newsletters.

Finally, I have also noticed that you undertake that every data subject has "*the possibility to unsubscribe easily and for free*".

The CNIL reserves the right, in case of new complaints, to use all of the powers assigned to it under the GDPR and the law of January 6th, 1978 as amended.

Yours Sincerely,

Marie-Laure DENIS

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	20 March 2019
LSA:	FR
CSAs:	AT, DE - Rhineland-Palatinate, DE - North-Westphalia, DE - Lower Saxony, DE - Saarland, DE - Mecklenburg-Western Pomerania, DE - Bavaria
Legal Reference:	Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12), Information to be provided where personal data are collected from the data subject (Article 13), Information to be provided where personal data have not been obtained from the data subject (Article 14)
Decision:	No violation
Key words:	Transparency, Privacy statement, Consent

Summary of the Decision

Origin of the case

The complaint concerned the information delivered to individuals visiting the controller's websites as well as the conditions for processing personal data for the purposes of direct marketing. It was alleged that the controller collects data for advertising purposes without having privacy statement on its websites.

Findings

Following examination of the complaint, a series of exchanges between LSA services and the marketing service of the controller took place. The controller updated the information delivered to individuals visiting its websites, in accordance with Articles 13 and 14 of the GDPR, by the publication of a document entitled 'General Data Protection Regulation (GDPR)'. The LSA noted controller's commitment in pursuing a consent campaign for the collection and the use of personal data for the purposes of direct marketing from data subjects, prior to sending newsletters.

Lastly, it was observed that the controller undertakes measures to ensure that every data subject has ‘the possibility to unsubscribe easily and for free’.

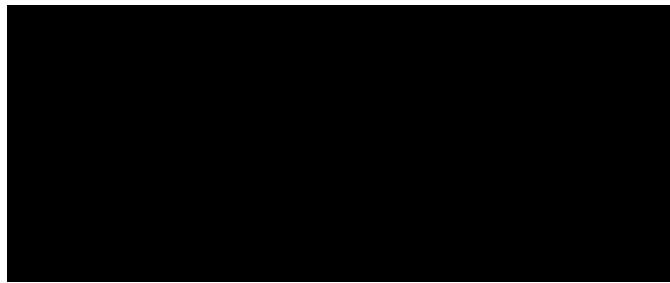
Decision

After having observed that the controller responded appropriately and demonstrated compliance with the GDPR, the LSA together with the CSAs agreed to proceed to the closure of the complaint.

Comments

Submitted by a citizen, but not a formal complaint (Art. 77 GDPR)

The President



Examination of the case:

Paris, on May 16th, 2019

Our Ref.: MLD/JLI/KKR/XD/DAU/CM191523

Case no. 18021443

(to be referenced in all correspondence)

Dear Mr. Chief Executive Officer,

This is further to the investigation carried out under decision no. 2018-268C on the premises of the [REDACTED] company on December 18th and 19th, 2018, whose purpose was in particular to examine the complaint transmitted to the French data protection authority ("CNIL") by the data protection authority of Hamburg according to provisions of Article 56.1 of the General Data Protection Regulation (GDPR) of April 27th, 2016.

Indeed, a complaint has been lodged with this authority against the [REDACTED] company concerning the fraudulent use of information relating to a room booked through [REDACTED] on September 1st, 2018, at the [REDACTED] for the night of September 8th/9th, 2018.

The elements resulting from this investigation lead me, in agreement with other European data protection authorities concerned by the processing carried out for the purposes of reservation management, **to proceed to the closure of this complaint**.

Indeed, first of all, it is observed that the [REDACTED] company was acting as a data processor for its hoteliers clients. [REDACTED] provides them tools for ensuring the management of their bookings, payments and issuing price recommendations. Agreements concluded with its hoteliers clients specifically indicate that data are "owned" by these hoteliers clients. Besides security measures, [REDACTED] adjusts the means of the processing it carries out in accordance with its clients' directives.

Secondly, the investigation revealed that the booking containing the personal data of the complainant (surname, first name and telephone number only) and addressed to different hotels was obviously false.

To begin with, several [REDACTED] hoteliers clients have noticed a booking clearly received on behalf of the complainant, but the e-mail address of the sender of this booking [REDACTED] is not the [REDACTED] one. In addition, the type of access link to banking data contained in this booking [REDACTED] is not consistent with the usual practice.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

As a result, a phishing attempt aiming to obtain credentials to [REDACTED] extranet remains the most probable hypothesis, although it cannot be ascertained.

The elements obtained during the investigation on your premises by the delegation of the CNIL did not allow establishing circumstances under which the personal data of the complainant could have been collected for being used in this operation. In view of the date of the facts, it is indeed not possible to ascertain these circumstances, but it remains likely that the [REDACTED] - with whom the complainant's booking was made - has been victim of a data breach. In this regard, I observe that you have used the procedure for modifying this hotel's password, on September 3rd, 2018, for it to keep on accessing to your services.

Furthermore, it is noted that on September 4th, 2018, the website hosting the false login pages for recovering login and password has been rendered inaccessible on [REDACTED] request.

Accordingly, the [REDACTED] company's liability for the facts reported in the complaint cannot be established under the findings established during the onsite investigations.

Yours Sincerely,



Marie-Laure DENIS

Summary Final Decision Art 60 Complaint

No liability of the processor

Background information

Date of final decision:	16 May 2019
LSA:	FR
CSAs:	AT, BE, DE-Hamburg, DE-Lower Saxony, DE-Bavaria (private sector), DK, EL, ES, IT, NO, PT, SK,
Legal Reference:	Art 6 Lawfulness of processing
Decision:	No liability of the processor
Key words:	Data breach, Lawfulness of processing, Security of processing

Summary of the Decision

Origin of the case

The case opened after a complaint was lodged regarding fraudulent use of information relating to a room booked on a booking website. The complainant had booked a hotel room on a booking website. Shortly after, the complainant was contacted by several hotels from different cities claiming to have received a hotel reservation through the booking website.

Findings

After the investigation, the LSA considers likely that the hotel where the complainant planned to stay had suffered a data breach. The LSA notes that the processor has used the procedure to modify the hotel's password, for it to keep on accessing the processor's services.

Decision

The LSA concluded that the processor's liability in this case couldn't be established.

Comments

The LSA initiated an Article 56 GDPR proceeding for the booking website.

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	17 June 2019
LSA:	FR
CSAs:	BE, ES, LU, DE-Lower Saxony, DE-Rhineland-Palatinate, DE-Berlin, IT
Legal Reference:	Security of processing (Article 32)
Decision:	No violation of art. 32 GDPR and recommendation on the adoption of technical measures
Key words:	Consumers, e-commerce, security of data

Summary of the Decision

Origin of the case

This case concerned a complaint lodged by a data subject regarding the fact that the username and password for access to a website operated by the controller were given to him via a plain text email.

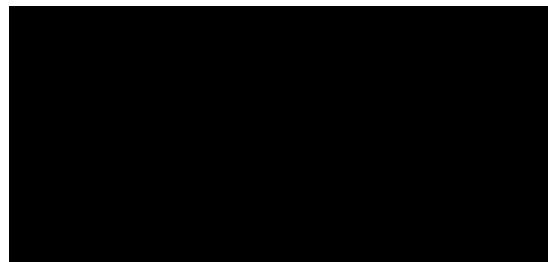
Findings

After correspondence with the controller, the LSA reached the conclusion that it did not communicate to its users or store in its databases plaintext passwords. However, the LSA found that, despite its assertions to the contrary, the controller did not operate a captcha system and only operated an access temporization system of 1 second.

Decision

The LSA closed the case regarding the complaint and recommended to the controller to introduce a captcha system and enhance access temporization to 1 minute after 5 failed attempts and introducing a limit of 25 attempts within 24 hours.

The President



Examination of the case :

Paris, on **13 JUIN 2019**

Our Ref.: MLD/JLI/XD/SGE/DAU/CM191944

Case no. 19001065

(to be referenced in all correspondence)

Sir,

This is further to the exchanges that took place between my services and yourself concerning the examination of the complaint lodged with the CNIL and examined in accordance with provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint was related to the conditions of processing of personal data of individuals that have created an account on the website [REDACTED]. More specifically, the complainant indicated having received his username and password in plain text by email following the creation of his account on this website.

These exchanges lead me, in agreement with other European data protection authorities concerned by the processing of data of individuals registered on [REDACTED] to proceed to the closure of this complaint.

Indeed, in view of materials submitted, I note that you do not communicate to your users, nor store in your databases plaintext passwords.

Nonetheless, I should like to draw your attention on the malfunction identified concerning security of your authentication means.

Indeed, you put forward your compliance with security measures regarding passwords. In this regard, I take note that these do have a length of at least 8 characters and have to include at least 4 categories of characters (uppercase, lowercase, numbers and special characters), as indicated.

Nonetheless, you specify using a «captcha» mechanism as a complementary measure. Yet, such mechanism did not stem from materials submitted. My services have thus proceeded to informal checks on your website. They have not observed any «captcha» mechanism at the stage of user authentication but only a measure of access temporization which does not appear to be sufficient. Indeed, they have noticed that following 8 unsuccessful login attempts, the login page displayed the following message: “*Too many login attempts. Please try again in 1 second*”.

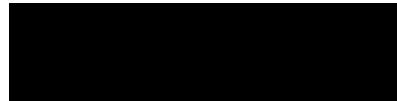
RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

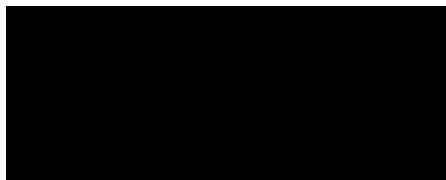
As a result, I invite you:

- to implement efficiently a « captcha » mechanism in order to prevent you from intensive and automated submissions attempts to login; and/or
- to enhance the measure of access temporization of 1 second currently on your website; the CNIL recommends in its deliberation no. 2017-012 of January 19th, 2017 the period of such measure to last more than 1 minute after 5 failed attempts, within a limit of 25 attempts per 24 hours.

Yours Sincerely,



Marie-Laure DENIS



Paris, on **09 AOUT 2019**

Examination of the case:

No./Ref: MLD/JLI/KKR/XD/EMT/CM192211
Request n°19004571
(to be recalled in any future correspondence)

Dear Mr. President,

This is further to the exchanges that took place between the CNIL's services and the data protection officer of your company in the framework of the examination of the complaint transmitted to us by the Spanish data protection authority according to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

This complaint was lodged by [REDACTED] who faced difficulties in exercising his right to object to receive marketing emails from [REDACTED].

Those exchanges are leading me, in agreement with the others European data protection authorities concerned by the processing carried out for the purpose of direct marketing, to proceed to the closure of this complaint.

Indeed, you mentioned that [REDACTED] initially agreed to receive the “[REDACTED]” newsletters when he asked for [REDACTED] in October 4 and 7, 2016, and I have noted that you have taken into account his request of objection by removing his data from your database.

Furthermore, your data protection officer mentioned that this complaint had highlighted an internal dysfunction due to a programming anomaly affecting your [REDACTED] Cloud Marketing tool, implemented since October 2018.

This dysfunction prevented from « taking into account the unsubscribing request made by an internet user within seven days after his initial subscription date to [your] newsletter ».

I have noted that this dysfunction has been corrected since March 29, 2019 and that any unsubscribing request is now taken into account regardless of the initial subscription date.

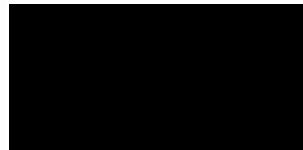
RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Finally, I have noticed that you are currently reviewing all the unsubscribing requests that you have received within seven days or less after the initial subscription date, since the implementation of your [REDACTED] Cloud Marketing tool in October 2018 until March 29, 2019, to make sure that all the deletion requests from your database have been taken into account.

The CNIL reserves the right, in case of new complaints, to use all of the powers assigned to it under the GDPR and the law of January 6th, 1978 as amended.

Yours Sincerely,



Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision: 9 August 2019

LSA: FR

CSAs: ES, IT

Legal Reference: Lawfulness of the processing (Article 6 GDPR)

Decision: No violation

Key words: lawfulness of the processing, right to object, spam emails, unsolicited communication, rights of the data subject

Summary of the Decision

Origin of the case

The complainant alleged he faced difficulties when he tried to exercise his right to object to unsolicited marketing emails.

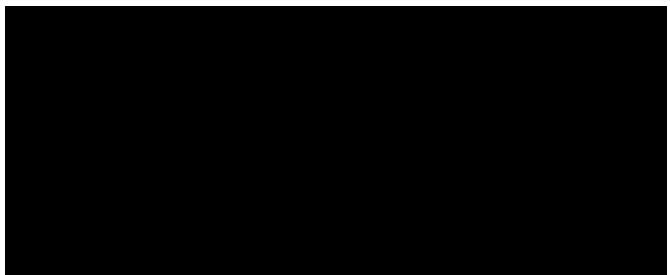
Findings

The LSA found that the complainant had consented to receiving marketing emails and that the controller removed the complainant's data from their database, following the request. The controller's reaction to the request was delayed, due to an internal dysfunction, which has since been resolved.

Decision

The LSA found no infringement.

The President



Examination of the case:

Paris, on **23 AOUT 2019**

Our Ref.: MLD/XD/SGE/DAU/CMI92505

Case no. 19005906

(to be referenced in all correspondence)

Dear Mr. Director General,

This is further to the exchanges that took place between the CNIL's services and the Legal department of the [REDACTED] (hereinafter the "████████") in the framework of the examination of the complaint of [REDACTED], which was transmitted to the CNIL by the German data protection authority of Saxony-Anhalt pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] had lodged a complaint with his national data protection authority against the [REDACTED] which would not have granted his objection request to receive direct marketing and his request to obtain access to data concerning him.

Those exchanges lead me, in agreement with other data protection authorities concerned by the processing for direct marketing purposes and for management of customers data purposes, to proceed to the closure of this complaint.

Indeed, in view of the materials submitted, I note that [REDACTED]'s requests have been granted.

I take note that [REDACTED]'s objection request dated July 14th, 2018 has been taken into account by your services on July 19th, 2018. At this time, the complainant's email address has been erased from your direct marketing tools and an unsubscribe confirmation message has been sent to him.

Nonetheless, I would like to draw your attention on the enhancements that must be brought to the unsubscribe process to [REDACTED]'s newsletters.

Indeed, the erasure of data from your systems requires a period of 24 to 48 hours to be effective within your systems.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

In view of these elements, I invite you to specify in your unsubscribe confirmation messages the existence of such period for requests to be effectively taken into account.

Yours Sincerely,



Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision: 26 August 2019

LSA: FR

CSAs: AT, BE, DE-Rhineland-Palatinate, DE-Saxony-Anhalt, DE-North Rhine-Westphalia, NL, UK

Legal Reference: Right of access (Article 15); Right to erasure (Article 17); Right to object (Article 21)

Decision: No violation of the GDPR

Key words: Right to object, right to access, direct marketing

Summary of the Decision

Origin of the case

The complainant alleged that the controller had not taken his objection to direct marketing into account and that his request to access his personal data had not been granted.

Findings

The LSA found that both requests had been granted. The complainant's email address had been erased from the controller's marketing tools and an unsubscribe confirmation message had been sent.

Decision

No violation of the GDPR was found.



Examination of the case :

No/Réf. : MLD/NLU/CMI 92254

Request n°18025015

(to be recalled in any future correspondance)

Dear Madam President,

This is further to the exchanges that took place between the CNIL's services and the service of your association in the framework of the examination of the complaint transmitted to us by the data protection authority of Belgium according to provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

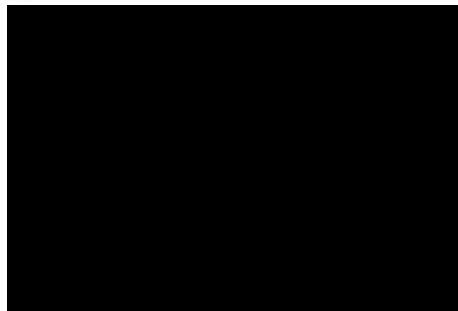
The complaint, submitted by [REDACTED], was dealing with the publication of her personal datas, without her consent, from the website [REDACTED]
[REDACTED].

Those exchanges are leading me, in agreement with other European data protection authorities concerned by your processing for customer loyalty, to proceed to the closure of this complaint.

Indeed, I have noticed, in your letter of 17 February 2019, that « *the anonymization of the first and last names contained in the aforementioned letters posted on the website [REDACTED] is done via black felting* ». I draw your attention on the fact that beyond this individual case, you're invited to anonymize the copies of the letters published on your website.

The CNIL reserves the right, in case of new complaints, to use all of the powers conferred to it under the GDPR and the law of January 6th, 1978 as amended.

Your Sincerely,



RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision: 29 August 2019

LSA: FR

CSAs: BE

Legal Reference: Right to erasure (Article 17), Right to object (Article 21)

Decision: No violation

Key words: Right to erasure, Right to object, Anonymisation

Summary of the Decision

Origin of the case

In a complaint filed with the CSA, the complainant alleged that personal data in her email correspondence with the controller was published on the controller's website without her consent.

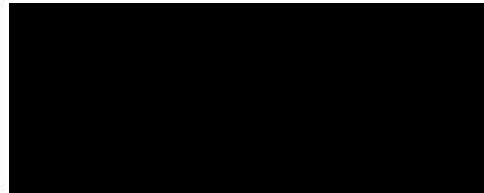
Findings

After communicating with the LSA, the controller took action to anonymise the complainant's first and last names from the correspondence.

Decision

The LSA invited the controller to anonymise the copies of all the letters published on its website. No further action towards the controller was taken.

The President



Registered letter with AR

N°2CJUR67468045

Examination of the case:

Paris, the **23 SEP. 2019**

Our Ref.: MLD/JLI/KKR/XD/APA/CLP191091

Case n°19002617

(to be referenced in all correspondence)

Dear Mr. Chief Executive Officer,

This is further to the email exchanges between my services and [REDACTED]'s Legal Director, concerning the complaint addressed to the CNIL by the Spanish data protection authority, in accordance with the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint concerned a request to delete a user account on the website<[REDACTED]>.

Those exchanges lead me, in agreement with other European data protection authorities concerned by the processing carried out by your company, to proceed to the closure of this complaint.

Indeed, it is noted that the request to delete a user account from the complainant has been taken into account in accordance with the article 17 of the GDPR.

Furthermore, I have taken notes of the explanation given on the payment data retention period, as provided in article L.133-24 of the Monetary and Financial Code, which specifies that "*The payment service user shall, without delay, report to his payment service provider an unauthorised or incorrectly executed payment transaction and at the latest within 13 months of the debit date under penalty of foreclosure unless the payment service provider has not provided or made available to him the information relating to that payment transaction in accordance with Chapter IV of Title I of Book III*". As a result, regardless the deletion of the complainant's user account, some information necessary to manage any claims and disputes related to a payment made on your platform are stored in an intermediate archive during a thirteen months period since the last payment made on the user account, and this, in accordance with Article 17(3) of the GDPR.

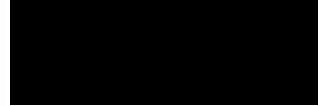
RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Finally, I have noticed that the complainant was directly informed by email on the 1st of April 2019 of the consideration given to his request, the need to keep some of his data and the date on which all his data will actually be deleted in their entirety.

The CNIL reserves the right, in case of new complaints, to use all of the powers conferred to it under the GDPR and the law of January 6th, 1978 as amended.

Yours sincerely,



Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	23 September 2019
LSA:	FR
CSAs:	DE-Mecklenburg-Western Pomerania, DE-Rhineland-Palatinate, ES
Legal Reference:	Right to erasure (Article 17)
Decision:	No infringement of the GDPR
Key words:	Right to erasure, Electronic communications, Payment data

Summary of the Decision

Origin of the case

The complainant asked for the deletion of his user account on the Spanish version of the controller's website. In its reply, the controller stated that it was required to keep some of his data. However, it informed the complainant of the date on which all of his data would be entirely deleted.

Findings

The LSA found that, pursuant to national law, the controller was required to retain the complainant's payment data in an intermediate archive upon the deletion of his user account in order to manage claims and disputes related to a payment made on its platform. In consequence, the controller acted in accordance with Article 17 (3) GDPR when it kept some of the complainant's data.

Decision

The LSA found that the controller complied with its obligations under the GDPR and closed the case.

Decision no. MED 2019-xx of xxxx issuing formal notice to the company

(No. MDM191003)

The Chair of the Commission Nationale de l’Informatique et des Libertés (French Data Protection Authority),

Having regard to Treaty no. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to the French Criminal Code;

Having regard to the French Postal and Electronic Communications Code;

Having regard to Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties, particularly Article 45;

Having regard to Decree no. 2005-1309 of 20 October 2005, amended, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation n°. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l’Informatique et des Libertés;

Having regard to decision n°. 2018-161C of 26 June 2018 of the Chair of the Commission Nationale de l’Informatique et des Libertés to entrust the Secretary General with carrying out an investigation on the company [REDACTED] or having such verification mission carried out;

Having regard to records of investigation n°s. 2018-161/1 of 31 July 2018 and 2018-161/2 of 25 October 2018;

Having regard to the other items in the case file;

I. Findings

The company [REDACTED] (hereinafter “the company”), located [REDACTED] [REDACTED] is a [REDACTED]. It employs [REDACTED] employees and, in 2017, generated revenues of around [REDACTED] for a net loss of around [REDACTED].

The company [REDACTED] markets [REDACTED]. Subscribers receive a [REDACTED] and [REDACTED] as well as digital access which enriches the magazine with a mobile app.

The company's products target a French customer base but are delivered to several countries, and particularly European countries. For the purposes of its activity, the company runs the [REDACTED] website (hereinafter "the Website"), through which customers can access their account and subscribe to the company's service. It also runs other versions of the website under national domain extensions (.ch, .co.uk, .be).

On 25 October 2018, the company appointed [REDACTED] as Data Protection Officer and notified the Commission Nationale de l'Informatique et des Libertés (hereinafter "CNIL" or "the Commission") (declaration n°. DPO-[REDACTED]).

In accordance with the decision of the Chair of the Commission no. 2018-161C of 26 June 2018, a CNIL delegation carried out on-site investigations on the company [REDACTED] on 31 July and 25 October 2018. Said investigations were aimed at confirming the compliance with Act n°. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties (hereinafter the "Data Protection Act" or "Act of 6 January 1978, amended") and with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "GDPR") of all of the personal data processing operations pertaining to the marketing and the use of products and services associated with the "[REDACTED]" brand.

By reproducing the account creation process on the company's Website, the investigation delegation found that when the user is asked to provide his/her name and surname, no information on the protection of his/her data is provided, and no link directs the user to the general terms and conditions of sale (hereinafter "the TCs").

On reading these TCs, the delegation found that these do not make any reference to the legal grounds for processing, the right to restriction of processing, to data portability or to the right to submit a claim to a supervisory authority.

On continuing the registration process, the delegation found that passwords are sent to customers in clear text via email. This email contains a link which redirects the user to the company's Website, and allows the user to customise their password. The delegation found that on this occasion a six-figure password such as "123456" was accepted.

After completing the registration process on the company's Website, the delegation found that, in the user account management window, the box corresponding to the option to receive newsletters and marketing emails was ticked by default.

At the bottom of this e-mail is a link to unsubscribe. A click on the link to unsubscribe redirects the user towards a webpage in English, with the title "*Unsubscribe From Messages From [REDACTED]*" and the following text: "*If you no longer wish for XXX to receive any email marketing message from [REDACTED] click Unsubscribe.*", in which XXX is the email address having received the marketing email.

By clicking on the button "*Unsubscribe*" below the text, the user is redirected to a second page, also written in English, containing the following text: "*The email address XXX has been unsubscribed from any future email marketing messages from [REDACTED] If you unsubscribed by mistake, you can re-subscribe by clicking here.*"

The delegation found that after creating an account on the company's Website, users could subscribe to the services offered by [REDACTED] or ask to receive a test kit. In both cases, the user must fill out a form and provide various elements of personal data, particularly data relating to the [REDACTED] receiving the kit. This form is not accompanied by any information on personal data protection nor by any link through which the user is invited to learn such information.

During the investigation, the delegation found that the erasure of data on an account can be requested by the customer from their account. These requests are processed by customer service using the [REDACTED] ticketing management software.

The delegation found that eighteen requests to delete accounts were listed in [REDACTED]. For at least one of these requests, customer service had answered the requesting individual that “[their] personal data [had] been erased” from the company’s databases. Yet, the delegation found that this statement was not accurate, and that the customer account still contained personal data in administrative tool [REDACTED] database (containing information relating to the customer and his/her orders) after stating that they had been erased.

During the investigations carried out, the delegation also found that the computer used by one of the database’s administrators to connect to the management tool was configured to never go into “sleep” mode. It also found that one of the company’s engineers connects to his Windows session using a six-character password. Lastly, it found that the company’s technical manager is able to log in to the ticketing management software by using the customer service manager’s account.

Finally, an analysis of the items communicated by the company following the investigation led the delegation to find that passwords were kept after being run through the [REDACTED] algorithm.

II. Breaches to the provisions of the General Data Protection Regulation

A breach of the obligation to inform data subjects

Firstly, the delegation found that no information relating to personal data protection is communicated in a direct manner upon registering on the company’s website or when placing an order. Furthermore, no link is provided to redirect the user to the company’s general terms and conditions of sale (hereinafter “the TCs”) or privacy policy.

Moreover, said privacy policy is only accessible indirectly, as no link on the website refers the user directly to said policy. To find it, the user must read the TCs. This latter document, as recorded on the day of the investigation, contains an Article 22 on personal data as well as an Article 27.4 which includes a link to the privacy policy.

As regards the obligation of accessibility of information set out in Article 12 of the GDPR, the Article 29 Working Party guidelines on transparency under regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, specify that “*the criteria “easily-accessible” means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it*”.

Thus, “*every organisation that maintains a website should publish a privacy statement/notice on the website. A direct link to this privacy statement/notice should be clearly visible on each page of this website under a commonly used term (such as “Privacy”, “Privacy policy” or “Data Protection Notice”). Positioning or colour schemes that make a text or link less noticeable, or hard to find on a webpage, are not considered easily accessible*”.

The data controller must above all take concrete measures to ensure that information is directly provided to the data subject or “*to actively direct the data subject to the location of it (e.g. by way of a direct link, use of a QR code, etc.). The data subject must not have to actively search for information covered by these articles amongst other information, such as terms and conditions of use of a website or app*”.

Secondly, regarding both the TCs and the privacy policy, the user of the company’s website is not informed of the legal grounds for processing, nor of his/her right to the restriction of processing and to data portability, or even or his/her right to submit a claim to a supervisory authority.

Nor is the user informed of the data retention period. The company’s privacy policy does indeed contain an indication stating that “*data will be kept for the period necessary to provide the service requested by the user, or as set out in the objectives stated in this document.*”

In this respect, the guidelines on transparency under Regulation (EU) 2016/679 (WP260 rev.01) adopted on 29 November 2017 and revised on 11 April 2018 explicitly provide in their Annex 1 that: “*the storage period [...] should be phrased in a way that allows the data subject to assess, on the basis of his or her own situation, what the retention period will be for specific data/purposes .It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods.”*

This constitutes a breach of Article 13 of the GDPR, which requires that the data subject be provided with a certain amount of information relating to the data processing carried out.

This is also a breach of Article 12 of the GDPR, which requires that the data controller “*take appropriate measures to provide any information referred to in Articles 13 and 14 [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]*”.

Thirdly, the delegation also found that the newsletter and marketing email sent by the company to its customers or users contains a link enabling them to unsubscribe from this mailing list.

A click on this link redirects users to a page containing text in English, with a button which must be clicked to confirm their unsubscribe, also written in English. Furthermore, the page finalising the process to unsubscribe contains a hypertext link titled “*clicking here*” which results in a new subscription to newsletters and marketing emails. The presence of this hypertext link, in English, is of a nature to mislead the user and to make him/her believe that he/she must click to unsubscribe, leading to his/her subscription once more without him/her necessarily being aware.

Yet, the website is drafted targeting an exclusively French audience and only offers French content, both on its website and in the leaflets that the company distributes. In this respect, the Article 29 Working Party guidelines on transparency under Regulation (EU) 2016/679, adopted on 29 November 2017 and revised on 11 April 2018, specify that “*the requirement that information is “intelligible” means that it should be understood by an average member of the intended audience*” and that “*a translation in one or more other languages should be provided where the controller targets data subjects speaking those languages*”.

This is a breach of Article 12 of the GDPR, which requires that the data controller “*take appropriate measures to provide any information referred to in Articles 13 and 14 [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]*”. This article also provides that “*the data controller shall facilitate the exercise of data subject rights under Articles 15 to 22*”.

A breach of the obligation to comply with the request to erase data

The delegation found that on the date of the investigation, requests to erase data were not systematically followed by the effective erasure of concerned customer or users’ personal data, for requests going back at least five months. It was also found that the company’s customer service had informed users that their personal data had been erased despite the erroneous nature of this statement.

Although certain data can be kept under legal requirements or for purposes of proof following a request for erasure, the keeping of unnecessary data despite a data subject exercising his/her rights is a breach of the provisions of Article 17 of the GDPR, which provides that “*the data subject shall have the right to obtain from the data 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*”.

A breach of the obligation to ensure the security of data

Firstly, as regards passwords, the delegation found that upon creating an account on the company’s Website, a seven-character password containing only lowercase and uppercase letters is sent to the user by email, in clear text. When changing the password received, a six-character password is accepted.

It appears from these elements that the security measures in place are not enough to ensure a sufficient level of security and confidentiality given that the passwords used to create a customer account are comprised of only two types of characters (digits and letters), and can be only six characters long.

In fact, authentication based on the use of an insufficiently complex password can lead to the associated accounts being compromised and attacked by non-authorised third parties. Yet, these accounts contain personal data.

Secondly, the delegation was informed that passwords are kept after being run through the [REDACTED] algorithm, which is now considered [REDACTED]

It arises from these elements that the company's password management policy does not include sufficient and stringent measures to ensure the security and confidentiality of the data to which they allow access.

As regards the locking of workstations, the delegation found that the computer used by one of the database's administrators to connect to the management tool was configured to never go into "sleep" mode. This configuration means that the user's session is never automatically locked after a prolonged period of no use, e.g. after the employee leaves his workstation, and that third parties can access the data processed on said computer.

As regards access to data, the delegation found that the company's technical manager is able to log in to the ticketing management software by using the customer service manager's account. The absence of specific identification does not make it possible to ensure access traceability or that data are accessed only by those persons responsible for processing said data as part of their job.

This constitutes a breach of Article 32 of the GDPR which provides that "*the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

A breach of the obligation to obtain the consent of a data subject targeted by a direct marketing operation via email

The delegation found that, upon registering on the company's Website, the user is automatically subscribed to newsletters and marketing emails, even in the case in which he/she has not taken out any subscriptions and is therefore not one of the company's customers.

This constitutes a breach of the provisions of Article 13 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector- which provides that "*the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent*" - and of the provisions of Article L.34-5 of the French Postal and Electronic Communications Code- which provides that "*direct marketing through automatic calling machines, facsimile machines (fax) or electronic mail that use the contact details of a natural person who has not given prior consent to receiving direct marketing through said media is prohibited*".

In the absence of an order placed by the data subject, the company cannot validly invoke the benefit of the exception created by these texts which allows for marketing without prior consent when the recipient's contact details have been collected from said recipient for a sale or the provision of a service when such direct marketing concerns similar products or services provided by the same natural or legal person.

Thus, the company must collect the specific consent of users prior to any electronic marketing operations.

In light of the above, the company [REDACTED] located [REDACTED] in [REDACTED] ([REDACTED]), is hereby given formal notice, within two (2) months from the notification of this decision and subject to measures it may already have adopted to:

-) **inform data subjects, pursuant to the provisions of Articles 12 & 13 of the GDPR, about personal data processing activities set up, and in particular:**
 - Z **provide users with this information in an easily accessible manner on the forms used to collect personal data**, e.g. by providing at the bottom of these forms information on the data controller's identity, on the purposes of the processing and on the rights of data subjects, and by inviting users to view full and detailed information through a clickable link;
 - Z **provide full information**, for example in the Website's privacy policy accessible on the [REDACTED] website, mentioning all of the required information set out in Article 13 of the GDPR;
 - Z **set up a procedure for unsubscribing from the newsletter and marketing email that is compliant** with the provisions of Articles 12 and 21 of the RGPD, which can be understood by the users in question, written in the relevant language (in French for users of the website located in France) to ensure its effectiveness;
-) **ensure, under the conditions set out in Article 17 of the GDPR, the effectiveness of all requests to exercise the right of erasure made by data subjects whose data are processed by the company, and in particular, for older company customers, the erasure of their data, subject to those that must be temporarily archived under legal and litigious obligations;**
 - Z setting up a restrictive policy as regards the passwords used by the website users, particularly in terms of complexity (minimum of 12 characters including at least one lowercase, one uppercase, one digit and one special character, if there are no additional measures) and storage by using a robust hashing algorithm);
 - Z no longer sending passwords in clear text by email, especially during creation of a user account;
 - Z ensuring that the company's workstations go to sleep without fail, requiring a password to be entered to log in to the session again;
 - Z setting up individual accounts specific to each person with access to the company's tools, not least the ticketing management software;
-) **do not process data for direct electronic marketing purposes without first having obtained the freely given, specific and informed consent of data subjects who are not customers of the company, pursuant to the provisions of Article L34-5 of the French Postal and Electronic Communications Code, not least by ensuring that prior consent is obtained (e.g.: box to tick) and by no longer targeting data subjects who have not given their consent;**

-) Justify, to the CNIL, compliance with all of the above requests within the time-limit set.

After this time-limit, if the company [REDACTED] has complied with this formal notice, this procedure shall be considered closed and a letter shall be sent to it to this end.

However, if the company [REDACTED] has not complied with this formal notice, a rapporteur shall be appointed and may request that the restricted committee issue one of the measures set out under Article 45 of the Act of 6 January 1978, amended.

The Chair



Summary Final Decision Art 60

Investigation

Compliance order

Background information

Date of final decision:	16 December 2019
LSA:	FR
CSAs:	BE, DE-Rhineland-Palatinate, DK, ES, IT, HU, LU, PL, PT, SE, SK
Legal Reference:	Transparency and Information (Articles 12, 13 and 14), Right to erasure (Article 17), Right to object (Article 21), Security of processing (Article 32)
Decision:	Order to comply
Key words:	Transparency and Information, Right to Erasure, Right to Object, Security of Processing, E-Commerce, Direct Marketing, Children, Consumers

Summary of the Decision

Origin of the case

The LSA conducted two on-site investigations at the controller's premises to audit the controller's compliance with the GDPR and tested the procedure set up by the controller to create an account.

Findings

The controller is a company offering subscription to educational magazines for children. On the basis of the investigation, the LSA found several GDPR infringements. First of all, several breaches of the obligation to inform data subjects, enshrined in articles 12 and 13 GDPR, were identified. No information relating to data protection nor link to the controller's Terms and Conditions was given to the data subjects upon registration or when placing an order. As a consequence, the information was considered to be not accessible enough. The Terms and Conditions did not include any information on the legal basis for processing, on the retention period and on the individual rights to restriction of processing, data portability, or to submit a claim to a supervisory authority. Although the target audience was French-speaking and the website is fully in French, the "unsubscribe" button in the newsletter and marketing emails was hyperlinked to a text in English, asking for confirmation. An additional hypertext link was included in the final page (titled "Clicking here"): this is misleading for the user, as clicking on such link actually resulted in a new subscription.

Secondly, a breach of the obligation to comply with the request to erase data was identified, as personal data was not erased systematically when requested by data subjects although there was no legal requirement to keep it and although users had been informed of the erasure of the data

Last, there was a breach of the obligation to ensure the security of data, concerning passwords, locking of workstations, and access to data. More specifically, the password requirements and methods for processing the passwords were found to be non-compliant with the obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, since authentication was based on insufficiently complex passwords and obsolete hash algorithms. Additionally, the computer used by one of the database's administrators was configured to never automatically lock or go on sleep mode. With regard to access to data, the absence of specific identification (i.e. the use of the same account by several people) made it impossible to ensure access traceability.

Decision

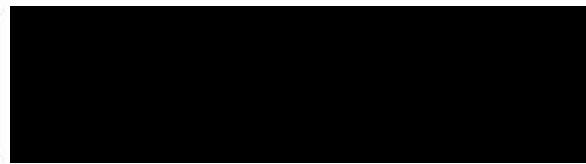
The LSA ordered the controller to comply, within two months of the notification of the decision, with several specific instructions.

First, the controller was ordered to provide full information to data subjects about the processing activities, in an easily accessible manner. Additionally, the LSA ordered the controller to set up a procedure for unsubscribing that is compliant with Articles 12 and 21 GDPR.

Secondly, the controller was ordered to ensure the effectiveness of all requests to exercise the right of erasure.

Last, the authority ordered the controller to take appropriate security measures to protect personal data and prevent access thereto by unauthorised third parties (by setting up a new password policy, avoiding the transmission of passwords in clear text, ensuring that workstations go on sleep mode, and setting up individual accounts).

The President



Examination of the case:

Paris, on 27 JAN. 2020

Our Ref.: MLD/KKR/XD/DAU/CM193696

Case no. 19006478

(to be referenced in all correspondence)

Dear Mr. Director General,

This is further to the exchanges that took place between the CNIL's services and the Data Protection Officer of [REDACTED] in the framework of the examination of the complaint lodged by [REDACTED], which has been transmitted to the CNIL by the Spanish data protection authority ("Agencia Española de Protección de Datos") according to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] had lodged a complaint with his national data protection authority against [REDACTED] which would have not granted his request to object to receive direct marketing as well as his request for account deletion.

These exchanges lead me, in agreement with the other European data protection authorities concerned by the direct marketing and customers' account management processing, to issue reprimands to you in accordance with the provisions of Article 58.2.b) of the GDPR.

Indeed, your services have not informed [REDACTED] about the effective deletion of his data.

Yet, in accordance with the provisions of Article 12.3 GDPR, the data controller is required to reply to the individual who made a request pursuant to Articles 15 to 22 GDPR, indicating the action taken further to his or her request without undue delay "and in any event within one month of receipt of the request".

Therefore, I hereby issue a reprimands to you on the need to respond to individuals making a request for the exercise of the rights within the legal time limit of one month, which may be extended by two further months where necessary, in particular in case of complexity of the request.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Moreover, you indicate that the unsubscribe link at the bottom of your direct marketing emails refers to the page "My communications" of the concerned customer account. As a result, prospects who do not have a customer account are unable to unsubscribe through this unsubscribe link. Therefore, I invite you to allow to unsubscribe directly following a simple click on this link, without referring to the concerned customer account.

In view of the information provided, however, I note that [REDACTED]'s customer account has been deleted a few days after 20 December 2018 and that the data concerning him have been erased from your direct marketing databases on 22 March 2019.

I also take note of the malfunction on your subsidiary's infrastructure which led to a lack of synchronisation between your direct marketing database and the [REDACTED] tool used to send emails to your members and thus explains the delay for taking into account [REDACTED]'s request to object.

Furthermore, I note that your services only request a copy of an identity document in the event of reasonable doubts concerning the identity of the applicant, in accordance with the provisions of Article 12.6 GDPR. In this case, since [REDACTED]'s account was already deleted when he objected on January 2019, your services requested such additional information in order to avoid any attempt of fraud or identity theft.

The CNIL reserves the right, in case of new claims, to use all of the powers conferred to it under the GDPR and the law of 6 January 1978 as amended.

Yours Sincerely,

[REDACTED]
[REDACTED]

This decision may be appealed before the French State Council within a period of two months following its notification.

Summary Final Decision Art 60 Complaint

Reprimand to controller

Background information

Date of final decision:	27 January 2020
LSA:	FR
CSAs:	AT, BE, DE, ES, IT, NL, UK
Legal Reference:	Transparency (Article 12), Right to erasure (Article 17), Right to object (Article 21)
Decision:	Infringement of the GDPR
Key words:	Erasure request, Objection, Direct marketing emails, Electronic communications, Reprimand

Summary of the Decision

Origin of the case

The complainant requested to have his account and personal data deleted and objected to the reception of direct marketing emails. According to the complainant, the controller did not comply with his requests.

Findings

The LSA found that, despite having deleted the complainant's account and personal data a few days after receiving the erasure request, the controller did not inform the complainant of the erasure.

Moreover, in order for the complainant to unsubscribe from direct marketing emails, he had to have an account with the controller's services. As his account was deleted, the complainant did no longer have the possibility to unsubscribe from direct marketing emails. However, the LSA found that the controller erased the complainant from the direct marketing databases, even though with a delay due to the lack of synchronisation between his direct marketing database and the tool used by his subsidiary to send emails to members.

Decision

The LSA found that the controller did not comply with his obligations under the GDPR and issued him a reprimand.

The President



Examination of the case:

Paris,

20 FEV. 2020

Our ref.: MLD/JLI/KKR/SGE/DAU/CMI93756

Case no. 19006155

(to be referenced in all correspondence)

Dear Mr. President,

This is further to the different exchanges that took place between the CNIL's services and the Data Protection Officer (hereinafter "DPO") of [REDACTED] in the framework of the examination of the complaint lodged by [REDACTED], transmitted to the CNIL by the data protection authority in Luxembourg ("Commission nationale pour la protection des données" ou "CNPD") according to provisions of Article 56.1 of the General Data Protection Regulation ("GDPR").

[REDACTED] had lodged a complaint with his national data protection authority against [REDACTED] concerning the difficulties encountered in the exercise of his right to object to receive direct marketing by text messages.

The breaches identified through the several exchanges between the CNIL and the DPO of [REDACTED] lead me, in agreement with the other European data protection authorities concerned by the processing for direct marketing purposes, to issue reprimands to [REDACTED], in accordance with the provisions of Article 58.2.b) GDPR.

First of all, I note the deletion of [REDACTED] telephone number from [REDACTED]' customer database has been duly made on September 12, 2018, as initially indicated by your services to the latter. I understand that the sending of direct marketing SMS on September 19, 2018 results from a processing carried out on September 13, 2018 by [REDACTED]' provider, on the latter's prior instructions. Mobile telephone numbers being erased within 48 to 72 hours, I take note that [REDACTED] now informs individuals exercising their right to object about the delay for such right to be effectively taken into account.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

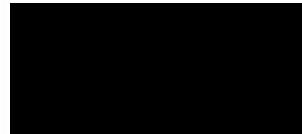
In addition, [REDACTED] complaint led to examine the "*Charter for data protection*" of the website <[REDACTED]> and thus revealed the fact that the latter systematically, for any requests to exercise rights, required to provide a copy of an identity document in breach of Article 12.6 GDPR and Article 92 of the French decree no. 2005-1309 of 20 October 2005 as amended. Nevertheless, I note that [REDACTED] has undertaken to adjust its procedure for requiring an identity document solely under specific circumstances, such as, for instance, a request submitted from an email address diverging from the one registered in the customer's personal space or a request requiring the transmission of numerous personal data. I also note that you will enable data subjects to exercise their rights directly from their personal space as from the second quarter of 2020.

Furthermore, I would remind that you have to, where appropriate, update regularly information in order to meet the objective of transparency, accessibility and clarity of the information delivered to individuals (Article 12.2 GDPR). In this regard, the information on appropriate safeguards in the event of data transfer outside the European Union delivered at the bottom of [REDACTED] direct marketing e-mails appears incomplete. Nevertheless, I note that [REDACTED] has answered making no such transfers to this day. Consequently, I draw your attention to the need to delete such reference for not misleading [REDACTED]'s customers and accurately reflecting the processing carried out. Furthermore, I notice that [REDACTED] has finally generally taken into account the remarks made by the CNIL on the need to improve the information delivered to individuals at the registration stage and when sending direct marketing messages (in particular by specifying the contact addresses for exercising rights).

Finally, within the examination of this complaint, I understand on the one hand that [REDACTED] offers to data subjects the opportunity to object to direct marketing emails at the collection stage of their data and when receiving direct marketing messages. On the other hand, I note that [REDACTED] does not transfer customer data to its partners for electronic direct marketing purposes.

The CNIL reserves the right, in case of new complaints, to use of all the other powers conferred to it under the law of January 6th, 1978 as amended and the GDPR.

Yours Sincerely,



This decision may be appealed before the French State Council within a period of two months following its notification.

Summary Final Decision Art 60

Complaint

Reprimand

Background information

Date of final decision:	20 February 2020
LSA:	FR
CSAs:	LU
Legal Reference:	Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12) Right to object (Article 21)
Decision:	Reprimand
Key words:	Right to object, E-commerce.

Summary of the Decision

Origin of the case

The complainant received SMS marketing on his phone. Following his objection to the controller, he received another marketing SMS.

Findings

The LSA has made note of the fact that there was a delay in deletion of the complainant's data of 48 - 72 hours. The controller will now inform individuals when exercising their right to object of the abovementioned delay.

Further, the LSA found out that the controller's procedure for requests to exercise rights required complainants to systematically provide a copy of an identity document, in breach of Article 12(6) GDPR. Also, the information delivered to individuals at the registration stage and when sending direct marketing messages did not meet the objective of transparency, accessibility and clarity as set out in Article 12.2 GDPR.

The controller undertook the necessary actions to adjust its procedure to request an identity document only under specific circumstances and to improve the information delivered to individuals at the registration stage and when sending direct marketing messages, for instance detailing the contact addresses for exercising rights.

Decision

The LSA issued a reprimand in accordance with Article 58(2)(b) GDPR.

The President



Examination of the case:

Paris, on **25 FEV. 2020**

N/Réf.: MLD/JLI/KKR/XD/EMT/CM192961
(to be recalled in any future correspondence)

Dear Mr [REDACTED]

I am writing to you further to the exchanges of emails between the CNIL and your company's Data Protection Officer (hereinafter referred to as "DPO") in the context of the investigation of six complaints relating to problems encountered by users of [REDACTED] website in exercising their rights as provided for by the General Data Protection Regulation (GDPR).

I should remind you that the six complaints bear on difficulties encountered during exercise of the right to object and rights of access and portability.

The elements resulting from these exchanges lead me, in agreement with the other data protection authorities concerned by the management processing of your platform's users, to issue reprimands to [REDACTED] regarding its obligations, in accordance with the provisions of Article 58.2.b) of the General Data Protection Regulation (GDPR).

Indeed, the investigation of the complaints has pointed out, on the one hand, that a technical problem arised during summer 2018 had prevented the taking account of the communication preferences of some users and, on the other hand, that the [REDACTED]'s methods of responding to its users' access requests were not compliant with the provisions of the GDPR (1).

That being recalled, I take note that [REDACTED] has taken measures to improve the process for managing requests for the exercise of rights (2). I also note the fact [REDACTED] has given a satisfactory outcome to requests of each complainant.

1. Reminder of your obligations under the GDPR

➤ On the technical problem affecting objection to direct marketing

The CNIL asked your DPO to specify the extent of the consequences of the technical problem highlighted in the context of the complaint investigation, as well as the measures [REDACTED] has taken to remedy the said problem.

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

→ On the technical problem's consequences

Your DPO stated that “during May 2018, [REDACTED] modified the presentation of product communication preferences with a view to enabling its users to give or withdraw their consent independently for each communication channel (email, SMS, and in-app messages or notifications) rather than there being a single choice for all channels.

- Such modification required (i) migration of communication choices previously made by users to communication categories redefined by [REDACTED] and (ii) synchronisation of such communication choices with [your] emailing tool so as to ensure that emails are only sent to users who have consented to receiving messages on [your part].

However, an incident arose during migration, with the following consequences:

- first of all, a mapping problem arose between the old and new consent management platform: where the old platform had assigned a “true” value to consents given and an empty value to consents not given/withdrawn, the new platform considered that empty values should be considered as “true” values (and not “false” as should have been the case);
- secondly, a synchronisation problem affected [your] emailing tool, preventing users’ communication choices from being taken into account during communication campaigns”.

I note that your DPO specified that the incident had not only affected users who had made communication choices prior to migration to the new consent management platform (mapping problem), but also those who had modified their choices following such migration (synchronisation problem).

→ On measures implemented in order to remedy the problem and restore users' communication choices

Your DPO stated that [REDACTED] took the following measures:

- “modification of the new migration script and application of the new script to all users registered before 25 May 2018;
- verification that users’ communication choices had been included in our emailing tool, so as to make sure that users targeted by our campaigns had actually given their consent;
- campaigns during summer 2018 to inform users of the change in communication preferences and ask them to configure their choices accordingly”.

If I take note of the fact that the problem has been solved and that users’ communication preferences have now been restored, the abovementioned facts lead me to remind you that Article 24 of the GDPR stipulates that “*taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure [...] that processing is performed in accordance with this Regulation.*“

This being so, it is [REDACTED] responsibility to implement appropriate technical and organisational measures to ensure that its users’ agreement or objection to receiving direct marketing are complied with.

Yet the facts outlined above show that [REDACTED] failed to fulfil its obligations as provided for by the GDPR, when, prior to migration of its consent management tool, it did not implement the necessary measures to take permanent account of and integrate its users’ choices.

➤ **On methods of responding to right of access**

Your DPO stated that when [REDACTED] received an access request to his/her personal data from a user, such request was followed up in accordance with the following procedure:

- creation of a folder dedicated to the user on an SFTP server belonging to [REDACTED],
- deposit into the folder of a file containing all data on the user in [REDACTED]'s possession,
- communication to the user of usernames enabling him or her to connect to the dedicated folder.

Your DPO stated that connection username and password were communicated to the user by a message sent set to his/her [REDACTED] personal space or, in the absence of a [REDACTED] account, by email to the address used to access the service.

In this respect, I should remind you that personal data must be used in such a way as to guarantee its security, in particular by ensuring that appropriate technical and organisational measures are taken (Article 5.1 (f) of the GDPR). The Data Controller must implement measures that guarantee the confidentiality, integrity and availability of data processed (Article 32 of the GDPR).

Yet, failing prior authentication, common communication of username and password for connection to content containing personal data via one and the same channel does not seem appropriate in view of these provisions, if data security is to be guaranteed.

It is the Data Controller's duty to communicate connection username and password via two different communication channels. In this particular case, if the link to the SFTP server and the connection username can be communicated to the person concerned by email, the password must be sent to him/her via another channel (for example, by asking the person to receive it by SMS, orally, by telephone, or by post).

On this point, it is your responsibility to modify your procedure for making data available in the context of requests for right of access, so as to ensure that it is in compliance with the GDPR.

2. Measures taken by [REDACTED]

Finally, the exchanges between the CNIL and your DPO made it clear that [REDACTED] has implemented procedures designed to better manage inflows of requests from data subjects regarding their rights guaranteed by the GDPR.

In this respect, your DPO stated that [REDACTED]'s customer service received an average of 10,000 customer requests a week, sometimes peaking at over 12,000 requests, and that about 10% of such requests related to users' personal data (access, portability, modification and deletion).

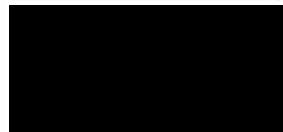
This being so, I note that [REDACTED] has implemented a special procedure for managing requests concerning its users' data, at the address "[REDACTED]". The requests received via this address are sent to [REDACTED]'s customer service and are the subject of intervention tickets in order to guarantee their follow-up and traceability.

Finally, I take note of the fact that [REDACTED] is also implementing one-off measures designed to improve its customer service's responses to users exercising their rights as provided for by the GDPR.

[REDACTED] O has told the CNIL that a GDPR workshop for customer support teams has been held in [REDACTED] designed to raise their awareness on the data protection question, train them in the procedure for responding to customers' requests, and identify avenues for improvement.

I would ask you to continue with these initiatives and must advise you that, in the event of any further complaints, the CNIL reserves the right to make full use of the powers vested in it by the GDPR

Yours Sincerely,



This decision may be appealed before the French State Council within a period of two months following its notification.

The President



Paris, on May 11th, 2020

Our Ref.: MLD/KKR/SGE/DAU/CM201158

Cases no. 19012057

(to be referenced in all correspondence)

Dear Mr. President,

This is further to the exchanges which took place between CNIL's services and [REDACTED] 's representatives in the context of the examination of [REDACTED] 's complaint, pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] lodged a complaint with the CNIL regarding the difficulties encountered with [REDACTED] to obtain the deletion of her personal data.

These exchanges lead me, in agreement with the other European data protection authorities that are concerned by the processing of data of [REDACTED] service's customers, **to issue reprimands to [REDACTED] on the following points, in accordance with the provisions of Article 58.2.b) of the GDPR.**

Indeed, [REDACTED] has to ensure and be able to demonstrate that its customers' data are being processed lawfully, fairly and in a transparent manner in relation to them (Articles 5.1.a) and 5.2 GDPR). In addition, pursuant to Articles 17.1 and 21.1 GDPR, when a customer of [REDACTED] asks for the deletion of his or her personal data, the latter shall have the obligation to erase these data without undue delay.

In this particular case, [REDACTED] still had access to her [REDACTED] account and to the data relating to her order history, despite confirmation by [REDACTED] 's services of the deletion of her account and of all her personal data by an email dated February 16th, 2019.

Yet, such confirmation should have been addressed to [REDACTED] only after that [REDACTED] has ensured itself that her data have been effectively deleted.

By a first response letter to the CNIL dated September 25th, 2019, [REDACTED] stated that the deactivation of [REDACTED] 's account, which took place though the day after her request (that is on February 16th, 2019), was not effective when she tried to connect to her former account with her [REDACTED] ID due to a technical malfunction. It specified that it had resolved this technical malfunction on September 17th, 2019 using a script that makes the deactivated accounts unavailable, unless specifically required by its authorized personnel.

— RÉPUBLIQUE FRANÇAISE —

3 Place de Fontenoy, TSA 80715 – 75334 PARIS CEDEX 07 – 01 53 73 22 22 – www.cnil.fr

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles.

However, as indicated by a second letter dated January 14th, 2020, [REDACTED]’s investigations revealed that along with these measures, a member of the customer service had previously taken the initiative to obfuscate the sole complainant’s account ID for trying to solve her difficulty. This initiative would have prevent the functioning of the script and overall, the deletion of the complainant’s account.

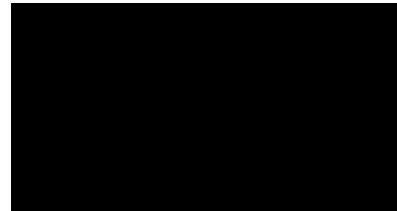
I note that challenged once more by CNIL’s services, [REDACTED] subsequently restored [REDACTED]’ account ID and restarted the script so that her account could effectively be unavailable.

It stems from the above that [REDACTED] has not been able to demonstrate the effectiveness of the deletion of [REDACTED]’ data, despite a first confirmation to her and then a second one to CNIL’s services.

Furthermore, I note that [REDACTED] has indicated that it will proceed with the definitive deletion of the complainant’s data at the end of the applicable limitation periods and retention obligations (in particular to respond to the risk of litigation or pursuant to Article L.123-22 of the French commercial code).

For all purposes, I thus draw [REDACTED]’ attention on the need to sort through [REDACTED]’ data in order to solely store, in intermediate archives with restricted access, data necessary for the exercise of legal claims or for compliance with legal obligations (see, to that effect, the fact sheet entitled “*Limit data retention*” available on CNIL’s website at the following URL: <https://www.cnil.fr/fr/limiter-la-conservation-des-donnees>).

Yours Sincerely,



This decision may be appealed before the French State Council within a period of two months following its notification.

Summary Final Decision Art 60

Complaint

Reprimand

Background information

Date of final decision:	11 May 2020
LSA:	FR
CSAs:	ES, PT, UK
Legal Reference:	Right to erasure (Article 17)
Decision:	Reprimand
Key words:	Right to erasure, Data retention

Summary of the Decision

Origin of the case

The data subject requested the controller to delete their personal data and received the controller's confirmation of the deletion of the data subject's account and their personal data. However, despite the confirmation, the data subject verified that he/she still had access to their customer account with the controller. Consequently, the data subject decided to lodge a complaint with the LSA.

Findings

In a first exchange of communications between the LSA and the data controller, the controller stated it had deactivated the complainant's account the day after their request, but that the deactivation was not effective when the complainant tried access the account due to a technical malfunction, which was only resolved months after. In a second letter, the controller reported that one the members of its customer service team had previously obfuscated the sole complainant's account ID to try to solve the data subject's difficulty, which prevented the functioning of the script and overall, the deletion of the account.

When the LSA inquired the controller for the second time, the controller had subsequently restored the complainant's account ID and restarted the script so that the account could effectively be unavailable. The LSA concluded that the controller had not been able to demonstrate the effectiveness of the deletion of the complainant's data, despite a first confirmation to the complainant and a second one to the LSA.

The controller indicated that it would proceed with the definitive deletion of the complainant's data at the end of the applicable limitation periods and domestic retention obligations.

Decision

The LSA reprimanded the controller on the need to sort through the complainant's data to store, in intermediate archives with restricted access, solely the personal data necessary for the exercise of legal claims, or for compliance with legal obligations.

The President

[REDACTED]
Mrs. President
74 RUE DE LA FÉDÉRATION
75015 - PARIS

Examination of the case:

Paris, on **03 JUIL. 2020**

Our Ref.: MLD/KKR/SGE/VEI/CM201945

Case n°19010704

(to be referenced in all correspondence)

Dear Mrs. President,

This is further to the exchanges that took place between the CNIL's services and the Data Protection Officer (DPO) of [REDACTED] in the context of the examination of a complaint lodged by [REDACTED] transmitted to us by the Danish data protection authority (Datatilsynet), according to Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] had lodged a complaint with his national data protection authority against [REDACTED] which didn't grant his access request.

The breaches identified through the exchanges between the CNIL and the DPO of [REDACTED] lead me, in agreement with the other European data protection authorities concerned by its processes, to issue reprimands to [REDACTED] in accordance with the provisions of Article 58.2.b) GDPR.

Indeed, in accordance with Articles 12 and 24 GDPR, [REDACTED] shall implement appropriate technical and organisational measures to facilitate the exercise of rights conferred on data subjects and to ensure that such requests for the exercise of rights are responded to within the time limit set by the GDPR.

However, the examination of this complaint has pointed out several malfunctions within your services.

In this present case, in order to explain the absence of response to [REDACTED] request, your DPO told the CNIL that the reference to a "*letter for your data controller*" in the complainant's request didn't allow your services to identify the right of access request, since the letter didn't mention key words, such as "GDPR, CNIL, data protection, personal data..."

Your DPO added that the right of access request was written in English, a language that is not professionally mastered by the team in charge of qualifying the mail. Nonetheless, the mail attached to the request was written in French and mentioned specifically that the request was intended "*for your data controller*".

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

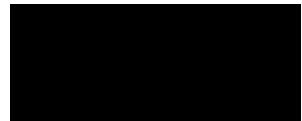
It appears from those explanations that the implemented measures didn't allow your teams to process data protection requests (identify the relevant requests, respect the deadlines, respond to requests...) and to ensure a simple and effective exercise of the rights of data subjects.

For an international company, offering benefits, services and products worldwide, the implementation of measures in order to deal with English requests seems to be a reasonable expectation, notably towards data subjects concerned by the processing.

Finally, I note that [REDACTED] request initiated on the 10th of December 2018, has been granted by [REDACTED] on the 2nd of July, 2019. To that extent, I remind you that according to Article 12 GDPR, even though you decide to extend the deadline for a response by two months to take into account the complexity of the request, you still have to reply to the data subject within a period of one month in order to inform that person of the extension and explain the reasons for it.

In closing, I would like to point out that the CNIL reserves the right, in case of new complaints, to use all the powers conferred to it under the law of January 6th, 1978 as amended, and the GDPR.

Yours Sincerely,



This decision may be appealed before the French State Council within a period of two months following its notification.

Summary Final Decision Art 60

Complaint

Reprimand to controller

EDPBI:FR:OSS:D:2020:120

Background information

Date of final decision: 03 July 2020

Date of broadcast: 03 July 2020

LSA: FR

CSAs: DK, SE, PL

Legal Reference: Right of access (Article 15)

Decision: Reprimand to controller

Key words: Consumers, credit, exercise of the rights of the data subjects, Finance

Summary of the Decision

Origin of the case

The complainant lodged a complaint with the CSA against the controller which did not grant his access request.

Findings

The controller informed the LSA that the reason behind the lack of response was due to the complainant's letter not mentioning the words 'GDPR', 'CNIL', 'data protection' or 'personal data'. The controller further added that the request of access was written in English, a language not professionally mastered by the team, although the mail attached was written in French.

The controller also took seven months to grant the request, despite the time limits set out under Article 12 GDPR.

Decision

The LSA will issue reprimands to the controller in accordance with Article 58(2)(b) GDPR. Further, in accordance with Articles 12 and 24 GDPR, the controller shall implement appropriate technical and organisational measures to facilitate the exercise of rights conferred on data subjects and to ensure that such requests are responded to within the time limit set by the GDPR.

Summary Final Decision Art 60

Complaint

Reprimand to the controller

Background information

Date of final decision:	25 February 2020
LSA:	FR
CSAs:	BE, DE Berlin, DE Hesse, DE Lower Saxony, DE Mecklenburg-Western Pomerania, DK, ES, FI, SE, UK
Legal Reference:	Responsibility of the controller (Article 24), Security of processing (Article 32)
Decision:	Reprimand
Key words:	Password, Right of access, Marketing preferences, Data security

Summary of the Decision

Origin of the case

The complainants have encountered difficulties during exercise of the right to object to direct marketing and rights of access and portability.

Findings

The LSA found out during the investigation that an incident arose during the migration of the controller's consent management tool for marketing communications, causing consents not given/withdrawn considered as given/not withdrawn, and the users' communication preferences not to be taken into account in the controller's communication campaigns.

Although the LSA noted that the problem had been solved and that the users' communication preferences had been restored, it stems from this incident that, prior the migration of its consent management tool, the controller had not implemented the necessary measures as required by the Article 24 GDPR

The LSA also found that the controller's procedure to process access requests was not fully compliant with the Article 32 GDPR. Indeed, the LSA noted that, in absence of a client account, the username

and password for connection to content containing data personal data were sent to data subjects via one and the same channel.

Thus, the controller has been asked to modify this procedure. The LSA determined that the controller had improved the procedures to handle data subject rights requests and trained employees on such procedures.

Decision

The LSA issued a reprimand to the controller.



Case No.: NAIH/2020/
Antecedent case No.: NAIH/2019/405.
In charge: [REDACTED]

[REDACTED]

[REDACTED]

Dear Sirs,

As you have already been informed by the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter: the Authority) based on the notification of [REDACTED] (hereinafter: the Complainant) an investigation was launched pursuant to Article 57(1)(f) of the General Data Protection Regulation (hereinafter: GDPR), and Section 38(3)(a) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act).

I. The course of the procedure

[REDACTED] (hereinafter: the Complainant) notified the Information Commissioner's Office of the United Kingdom (hereinafter: ICO), complaining that he requested [REDACTED] (which has since been transformed into [REDACTED] (hereinafter: the Company)) in vain to erase the user account registered with his e-mail address as the Company failed to meet his request.

On 8 December 2018, ICO initiated a procedure to determine the lead supervisory authority and the supervisory authorities concerned according to Article 56 of GDPR. In the course of this, it was established that the lead supervisory authority in this case is the Authority as the decisions concerning the purposes and instruments of processing personal data are made in Hungary within the Company's organisation.

To clarify the statements in the complaint, the Authority called upon the Company to make a statement on 7 February 2019 and at the same time, notify the Complainant electronically using the e-mail address [REDACTED], as well as by mail that an investigation was launched in the case.

The Company received the request of the Authority on 15 February 2019, and it requested the Authority to extend the deadline on 17 February 2019. The Authority granted the request of the Company and extended the deadline of responding until 12 March 2019. The statement of the Company was received by the Authority on 13 March 2019.

Based on the statement of the Company, clarification of additional issues were deemed necessary by the Authority, hence it called upon the Company to make additional statements in its letter of 18 June 2019, which the Company received on 26 June 2019. The Company requested an extension of the due date for responding by 15 days on the same day. The Authority granted the request and specified the deadline for responding as 31 July 2019. The Company's statement was received by the Authority on 29 July 2019.

II. The facts of the case

In his complaint lodged with ICO, whose exact date is not known to the Authority, the Complainant presented that he was unable to create a [REDACTED] account with his name and e-mail address, because his e-mail address was already in use. Earlier, his wife registered an account – [REDACTED] – using his e-mail address in the name of his mother-in-law when she bought a [REDACTED] for her from the Company.

The Complainant first requested the Company to erase the user account registered with his e-mail address in a letter sent to the e-mail address [REDACTED] by e-mail on 22 March 2018 as that account was not his. A customer service staff member of the Company informed him of having indicated the problem to their IT Department and the account would be erased within a few days; however, no measure of merit took place thereafter and the account was not erased. In an e-mail sent to [REDACTED] on 30 June 2018, the Complainant indicated that the account whose erasure he had requested was still active. In an e-mail of 9 July 2018, the customer service staff member informed him that he would again take up contact with the IT Department to erase the account. In his letter of 15 July 2018, the Complainant requested the Company to notify him of the erasure as he would like to buy a [REDACTED].

On 30 July 2018, the Complainant logged in to account No. [REDACTED] and lodged a complaint with the Company on account of not having complied with his request to erase.

In relation to account No. [REDACTED], the Company processed the following data:

- e-mail address: [REDACTED]
- name: [REDACTED]
- address: [REDACTED]
- phone number: [REDACTED]
- IP address: [REDACTED]

The account No. [REDACTED] was erased on 25 October 2018, but as a result of an administrative error, the Company failed to inform the Complainant of this, and he was informed of that only on 7 December 2018 after contacting the Company again on e-mail address [REDACTED] on account of erasing the account on 6 December 2018.

III. The findings of the Authority

III.1. Applicable legal regulations

The General Data Protection Regulation became applicable as from 25 May 2018. The Complainant lodged his first request for erasure with the Company on 22 March 2018, hence on the basis of this request to erase, the Authority is not entitled to adjudge the appropriateness of the measures taken by the Company or the failure of taking measures as a lead supervisory authority according to Article 56(1) of GDPR.

The Complainant's query of 30 June 2018 can, however, be interpreted as a repeated or maintained request to erase, which took place after GDPR became applicable, thus the measures taken by the Company can be evaluated according to the provisions of GDPR on that basis.

III.2. The right of the Complainant to erasure and evaluation of the request

III.2.1. The extent of the right to erasure due to the Complainant

Pursuant to Article 4(1) of GDPR personal data means any information relating to an identified or identifiable natural person; an identifiable natural person is one, who can be identified directly or

indirectly in particular by reference to an identifier, such as a name, identification number, location data, an online identifier or to one or more factors specific to that natural person.

There is no doubt that the e-mail address registered with the user account qualifies as the personal data of the Complainant, but the additional data recorded for the account are not data that can be related to the complainant; the Complainant is not identifiable on their basis. Therefore, the Complainant could only have requested the erasure of his e-mail address, not that of the entire account.

When submitting his request for erasure, the Complainant presented that it was not him who gave his e-mail address at the time of the registration of the account, it was not him who disposed of his personal data, i.e. his right to informational self-determination was violated already when his e-mail address was given to the Company.

Pursuant to the Company's Privacy Statement and their statement, the Company processes the personal data provided in the course of the registration of the account in accordance with Article 6(1)(b) of GDPR.¹ The contractual legal basis can be rightfully applied, if the data subject is party to the contract. In relation to the registration of account No. [REDACTED], the Complainant was not a party, also substantiated by the fact that he requested the erasure of the account and his e-mail address in order to be able to register an account for himself, i.e. to enable him to enter into contract with the Company.

The Company processed the e-mail address of the Complainant in the period from the registration of account No. [REDACTED] until the Complainant's request to erase through no fault of its own and without a legal basis, but the Company learned of the illegal data processing upon receipt of the first request to erase from the Complainant on 22 March 2018.

Pursuant to Article 17(1)(d) of GDPR, the data subject is entitled to request from the controller erasure of his personal data without undue delay and the controller has the obligation to erase the personal data without undue delay when the personal data have been unlawfully processed. Hence the Complainant had the right to request the erasure of his e-mail address from the Company.

III.2.2. Compliance with erasure requests by the Company

In spite of its promise, the Company did not take any action as a result of the Complainant's request of 30 June 2018, which can be taken into account in the course of the procedure as a repeated request for erasure within one month from lodging the request. Having logged in to the user account, the Complainant repeatedly requested the erasure of this account on 30 July 2018 presenting the antecedents of the case. The Company finally erased the account on the basis of the request submitted through the user account on 25 October 2018.

Consequently, the Company breached Article 12(3) of GDPR as it failed to take any action within a month from receiving the erasure requests, and after having erased the account, it failed to notify the Complainant of the erasure as its action taken for an additional one-and-a-half months until the inquiry by the Complainant.

Beyond this, the Complainant's right to erasure according to Article 17(1) of GDPR was also infringed as the Company complied with the erasure requests only with a substantial delay even though it

¹ The Authority did not examine the lawfulness of the applicability of Article 6(1)(b) of GDPR in the current procedure.

should have immediately erased the inaccurate personal data registered for the user account linked to his e-mail address according to Article 5(1)(d) of GDPR.

IV. Legal consequences

The Authority establishes that the Company has breached Article 12(3) of GDPR, when it failed to take action within a month on the basis of the Complainant's erasure request and when it failed to notify the Complainant of the fact of the erasure.

The Authority also establishes that the Company has breached Article 17 of GDPR as it met its erasure obligation only with a substantial delay.

The Authority – based on the Article 58(2)(b) of GDPR – issues a reprimand to the Company for the abovementioned infringements of GDPR.

In view, however, of the fact that the Company did erase the Complainant's user account on 25 October 2018 and it did notify the Complainant thereof on 7 December 2018, the Authority will not apply additional legal consequences and terminates the investigation on the basis of Article 53(5)(b) of the Privacy Act as the circumstance giving rise to conducting the investigation no longer exists.

Budapest, 29th June 2020.

Yours sincerely,

Dr. Attila Péterfalvi
President
Honorary university
professor



Case no.: NAIH/2018/4495/ /V

Subject: Final Decision

Official in charge: [REDACTED]

Attachment: Notice no.: NAIH/2018/4495/ /V

The regulatory inspection launched by the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) on 18th of July 2018, in relation to the obligations of [REDACTED] (hereinafter referred to as Controller or Group) based on Articles 33-34 of the Regulation (EU) 2016/6791 ('GDPR') concerning the data breach notified to the NAIH on 7th of July 2018, was closed by the Authority with the attached notice.

Please note that, based on Section 20 (1) of General Public Administration Procedures (hereinafter referred to as Ákr. Act), the official language in administrative proceedings is Hungarian, therefore the official version of the notice is the Hungarian, attached to this letter. However, in order to facilitate and accelerate the procedure, we hereby provide you with the summary of the relevant provisions of the notice in English language, for your information.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

On 18th of July 2018, the NAIH launched a regulatory inspection in relation to the data breach notified by the Controller, since the information given in the notification was not sufficient to assess whether the Controller had fully complied with the provisions of Articles 33-34 of the GDPR.

Based on the data breach notification and the Controller's answers to the questions asked by NAIH, the following could be established.

The Controller notified the NAIH on 7th of July 2018 that on 4th of July 2018 an attacker gained access to an employee's e-mail account and thus to the contact information - such as name, e-mail address and telephone number - of app. 800 colleagues, stored in the Controller's e-mail system.

The attacker was able log-in to the [REDACTED] e-mail address through the online available Outlook Web Application (OWA). In response, [REDACTED] Group Cyber Defence Centre (CDC) initiated its standard investigation and response process to contain the incident and understand the scope of the event.

The Group's network and system infrastructure was not compromised, the attack was limited to one e-mail account and its content. The forensic review conducted by the Controller's CDC professionals determined that the attacker viewed only a part of the contact list and e-mails. Based on the Controller's current understanding and the fact that the attacker tried to send out numerous e-mails, the attacker's primary goal was to use the compromised e-mail account to initiate a spam campaign. The spam campaign had a very limited effect due to the fact that the Controller's e-mail infrastructure only allows to send out a limited number of e-mails during a given time period. Following the detection of the attack, an internal e-mail was sent by the Controller, calling all colleague's attention to the phishing campaign.

[REDACTED] Group's Cyber Defence Centre disabled the compromised e-mail account, thereby removing the user from the e-mail system as soon as the incident was identified. A group of information security and data protection professionals assessed the situation and determined the necessary actions. The

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

account holder, whose account had been compromised, was given a new e-mail address and user name, and was also requested to change his passwords if he used it in his other accounts.

The rollout of multifactor authentication for Outlook Web Application is underway by the Controller. The implementation of this security measure will give an elevated level of security, ensuring that unauthorized access with a compromised password will be impossible without a second authentication factor which confirms the user's identity.

The data breach affected several colleagues residing in Member States other than Hungary. These Member States and the corresponding number of data subjects affected in that Member State are as follows: Austria – 1 person, Czech Republic – 4, Germany – 1, United Kingdom – 3, Croatia – 46, Italy – 14, Poland – 3, Romania – 11, Slovenia – 1, Slovakia – 68). The individuals affected were notified about the breach in their native language on 18th of July by the Controller.

Based on the circumstances of the case and the measures adopted by the Controller before and after the data breach occurred, the NAIH concluded that the Client has fulfilled its obligation under Articles 33-34 GPR concerning the data breach, and the procedure did not reveal any reasons to open administrative proceedings as described in Section 60 of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ('Privacy Act').

According to Section 38 (2) of the Privacy Act, the Authority shall be responsible to oversee and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest, and to ensure the free flow of personal data within the European Union. Section 38 (2a) of the Privacy Act, – which is also applicable in this procedure – provides that the powers and responsibilities conferred upon the supervisory authority by the GDPR shall be exercised with respect to the legal entities falling within the scope of Hungarian law by the Authority in accordance with the General Data Protection Regulation, and with the provisions laid down in this Chapter and in Chapter VI.

According to Article 2 (1), the GDPR is applicable to the data breach notified to the NAIH. Based on Section 99 of Ákr. Act, the NAIH - within the scope of its competence - shall monitor compliance with the provisions of legislation, and the implementation of enforceable decisions.

Based on Section 7 and 98 of Ákr. Act, the provisions of the Act on administrative proceedings shall apply to regulatory inspections subject to the derogations set out in Chapter VI of the Act. According to Section 100 (1) of the Ákr. Act, regulatory inspections are opened ex officio and conducted by the authority in own motion proceedings.

According to Section 101 of Ákr. Act, where the regulatory inspection finds any infringement, the authority shall open proceedings, or if the infringement uncovered falls within the jurisdiction of another body, the authority shall initiate the proceedings of that body. Where the authority finds no infringement during the regulatory inspection conducted at the client's request, it shall make out an official instrument to that effect. In the own motion regulatory inspections, the authority shall issue an official instrument on its findings at the client's request.

Budapest, " " of September 2018

On behalf of [REDACTED] president of the NAIH:

Summary Final Decision Art 60

Legal obligation

No infringement

EDPBI:HU:OSS:D:2020:116

Background information

Date of final decision:	N/A
Date of broadcast:	23 June 2020
LSA:	HU
CSAs:	AT, DE, IT, SI, SK
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No infringement
Key words:	Data breach, Electronic communications, Employment, Identity theft, Spam

Summary of the Decision

Origin of the case

The controller informed the LSA of the personal data breach.

Findings

An attacker had gained access to an employee's email account, and therefore the contact information of approximately 800 colleagues. The attacker was able to log in via an online email application. In response, the controller's cyber defence centre initiated its standard investigation and response process to contain the incident and understand the scope of the event.

The controller's group network and system infrastructure was not compromised as the attack was limited to one email account. The forensic review conducted by the controller determined that the attacker viewed only a part of the contact list. It is understood that the attacker tried to send out numerous emails. This spam campaign had had very limited impact due to the fact that the controller's email infrastructure only permits a small number of emails to be sent during a given time period. Following the detection of the attack, an internal e-mail was sent by the controller, informing colleagues of the phishing campaign.

The compromised email account was disabled. A rollout of multifactor authentication is currently underway which will give an elevated level of security.

Decision

Based on the circumstances of the case and the measures adopted by the controller before and after the data breach occurred, the LSA concluded that the controller had fulfilled its obligations under the GDPR, and the procedure did not reveal any reasons to open administrative proceedings.

Summary Final Decision Art 60

Complaint

Reprimand to controller

EDPBI:LSA:OSS:D:2020:118

Background information

Date of final decision:	29 June 2020
Date of broadcast:	02 July 2020
LSA:	HU
CSAs:	BE, CZ, DK, ES, FR, IT, NL, NO, UK
Legal Reference:	Right to erasure (Art 17)
Decision:	Reprimand to controller
Key words:	Consumers

Summary of the Decision

Origin of the case

Complainant lodged a complaint with one of the CSAs as the controller had not complied with his erasure requests.

Findings

The complainant was unable to create an account on the controller's website as his wife had already used his email to register an account.

After his first erasure request, a customer service representative of the controller informed him that the IT department would erase the account within a few days. After a number of months, the complainant emailed the controller to indicate that his erasure request was still active. He was informed again that the IT department would erase his account.

Following a number of months, the account was erased on the request of the complainant. As a result of an administrative error, the data controller failed to inform the complainant about the deletion, the complainant was only made aware of this after contacting the controller two months later.

As the complainant's second request was made following the implementation of the GDPR, it may be evaluated according to those provisions.

Decision

The controller breached Article 12(3) GDPR as it failed to take any action within a month of receiving the erasure requests, and after having erased the account, it failed to notify the complainant. Moreover, the complainant's right to erasure under Article 17 has been infringed.

The LSA issued a reprimand to the controller on this basis.

As the controller did erase the complainant's account and did notify the complainant thereof, the LSA will not apply additional legal consequences and will terminate the investigation.

Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

Reference is made to the complaint (registered internally with file number CDP/IMI/LSA/4/2019) received from the Data Protection Commission of Ireland concerning [REDACTED] (“the complainant”) who is alleging that [REDACTED] the controller“ or “the Bank” breached her data protection rights, as enshrined under the General Data Protection Regulation – Regulation (EU) 2016/679 (“GDPR” or “the Regulation). The complainant contended that the controller did not accede to the right of access request made to the personal data processed about her and also that the exercise of her right of erasure was not entirely satisfied.

INVESTIGATION

As part of the investigation process, through an email dated 20th December 2018, the Commissioner requested the controller to put forward its submissions on the allegation raised by the complainant. Submissions were received on the 21st of December 2018 and included the following principal arguments:

- the right of access and right of erasure requests were first received by the controller on 23rd September, 2018. On the 24th of September [REDACTED] cknowledged the complainant’s request and informed her that “*there may be the need to undergo an identification process*“. This process was required since [REDACTED] first communication with the Bank was made by using an email address that does not pertain to the data controller. The controller made several attempts to verify the complainant’s identity by sending her five (5) emails, between the 22nd of October and the 20th December 2018, but no reply was forthcoming. It is to be noted that [REDACTED] last communication with the Bank was on 2nd October 2018. All the personal data concerning the complainant being processed by the controller, including copies of the relevant documents, are ready to be sent to [REDACTED] nee the Bank is able to verify her identity;
- through an email dated 12th December 2018, the controller gave the complainant different options to confirm her identity as follows: a telephone number, a valid identification card to be sent by email, a skype call.

- there is a “Compromise Agreement” between [REDACTED] and the complainant which is and will remain valid when taking into account that it contains ongoing and biding obligations between the parties;
- the controller complied with the right of erasure request to the extent allowed by the above-mentioned “Compromise Agreement” and as per [REDACTED] data retention policy;
- the complainant’s HR file has been segregated with access to key persons only.

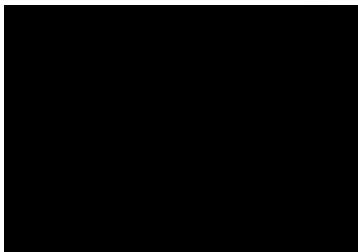
DECISION

On the basis of the foregoing and when taking into consideration:

- that, in terms of Recital 64 of the GDPR, “the controller should use all the reasonable measures to verify the identity of a data subject who submits a right of access request;
- that the Bank took all the necessary steps to handle the complainant’s right of access and the only reason why the information was not provided to [REDACTED] evolves around her failure to verify with the Bank her identity, given that she was using an email address that was not known to the Bank;
- that, Article 17.3 of the GDPR provides for the non-applicability of the data subject’s right to have personal data concerning him or her erased by the controller, in particular, when the processing is necessary for compliance with a legal obligation to which the controller is subject;
- that the Bank satisfied the complainant’s right of erasure request to the extent permissible by the applicable laws, including but not limited to, employment legislation;

The Commissioner hereby decides that the controller did not infringe the provisions of the Regulation and, consequently the complaint is dismissed.

A copy of this decision is also being sent the Data Protection Commission of Ireland.



Information and Data Protection Commissioner

Today, the 4th day of March, 2019



**RE.: IMI Case Register n.62564 - IMI Art.56 n.51645 - Complaint of [REDACTED] against [REDACTED]
- Final Decision**

Dear colleagues,

pursuant to Article 60(3) of the Regulation (UE) 2016/679 (hereafter GDPR), the Italian Supervisory Authority (hereafter Garante or ItSA) submits to you the following draft decision with regards to the abovementioned case.

[REDACTED], a German citizen, lodged a complaint with the Deutch Supervisory Authority of Baden-Württemberg stating that on 5 September 2018 he asked to the Italian controller, [REDACTED], the erasure of all his personal data, but the day after he received another SPAM e-mail.

Based on that complaint, the Garante requested the controller, an Italian [REDACTED] agency [REDACTED]
[REDACTED] to provide his comments about the processing of the complainant's data.

[REDACTED] sent the requested information within the deadline, voluntary translating the document both in English and in German.

The controller explained that [REDACTED] sent the erasure request by e-mail to the address [REDACTED] instead of to the dedicated e-mail [REDACTED] pointed out in the marketing e-mail footer. The mistake slowed the erasure procedure. Notwithstanding this, the user's request had been taken in charge very quickly and [REDACTED] had not received further marketing communication since 11 September 2018. The controller also assured that it takes care of the users' requests and it undertakes to reply as soon as possible.

According to the above-mentioned explanations, the Garante assumes that, in the present case, there is no infringement of the data subject right under Article 17 of the GDPR.

As a matter of fact, the complainant's erasure request had been taken in charge and dealt in few days. While Article 17 provides that the controller shall have the obligation to erase personal data "without undue delay", technical processing times are unavoidable. Moreover, in the present case, a special importance has to be accorded to the fact that the data subject enforced his right to erasure writing to the wrong e-mail address.

In view of the foregoing, the ItSA states that the complaint should be dismissed.

Please, submit your comments, if any, or your relevant and reasoned object to this draft decision within the four weeks obligatory timeframe pursuant to Article 60(4) of the GDPR.

On behalf of the ItSA
[REDACTED]



Summary Final Decision Art 60

Complaint

No ongoing infringement of the GDPR

Background information

Date of final decision: 17 September 2019

LSA: IT

CSAs: DE-Baden-Württemberg, DE-Hamburg, DE-Rhineland-Palatinate

Legal Reference: Right to erasure (Article 17)

Decision: No ongoing infringement of the GDPR

Key words: Right to erasure, Spam, Newsletter

Summary of the Decision

Origin of the case

The complainant sent an email to the controller to unsubscribe from a newsletter. The day following the erasure request, he received another SPAM email from the newsletter.

Findings

The LSA found that, instead of sending the erasure request to the dedicated email address present in the marketing email footer, the complainant sent it to the wrong email address, thus slowing down the procedure. Despite the complainant's mistake, the controller dealt with the erasure request within a few days.

Decision

The LSA found that the controller ultimately complied with his obligations under the GDPR, since some technical processing times are unavoidable especially if the data subject enforces his right writing to the wrong e-mail address, and dismissed the complaint.

Summary Final Decision Art 60

Complaint

Compliance order to controller

Background information

Date of final decision:	21 August 2019
LSA:	LI
CSAs:	DE-Lower Saxony
Legal Reference:	Principles relating to processing of personal data (Article 5), Lawfulness of processing (Article 6), Conditions for consent (Article 7), Right of access by the data subject (Article 15), Security of processing (Article 32)
Decision:	Compliance order to controller
Key words:	Consent, Transparency

Summary of the Decision

Origin of the case

The complainant lodged a complaint with the Commissioner for Data Protection of Lower Saxony, alleging he received unsolicited personalised advertising. In its reply to the data subject's right of access request, the controller had stated that the complainant's personal data was the result of a prize competition in which he had allegedly participated consenting to the use of his data for marketing purposes by the controller or its sponsors.

Findings

In its assessment of the validity of the consent provided by the complainant, the LI SA found that the text explaining the checkbox for consent was inconsistent with the privacy policy, which referred to a wider range of processing activities and a larger number of recipients: thus, the consent was not legally valid and Articles 5(1)(a), 6 and 7 GDPR were violated.

Furthermore, the LI SA found that the controller did not comply with Article 15 GDPR as it did not appropriately provide the data subject with information on the purposes of the processing of personal data, the recipients and the storage period.

In addition, violations of Article 32 GDPR were also identified: first, the technical and organizational measures implemented by the processor (e.g. double opt-in procedure) were not sufficient to prevent the misuse of personal data; secondly, the unauthorized entry of data could not be traced back due to the deletion of the link relating to the generated lead after a 30-day period.

Decision

The LI SA required the controller to take the following required steps within three months:

- seek consent in accordance with Article 7 GDPR and revise the Terms and Conditions and Privacy Notice of the prize competition;
- implement further technical and organisational measures;
- ensure that the author or source of the manipulation can be identified.



DATENSCHUTZSTELLE
FÜRSTENTUM LIECHTENSTEIN

Aktenzeichen: 103.1.2 2018-774

Beschwerdeführer:

[REDACTED]

Beschwerdegegnerin:

[REDACTED]
[REDACTED]
[REDACTED]

wegen:

Verletzung von Art. 5, 6 und 7 DSGVO

VERFUEGUNG

SPRUCH

Die Datenschutzstelle Liechtenstein entscheidet über die Beschwerde vom 25. Mai 2018 von

[REDACTED] (Beschwerdeführer)

gegen

[REDACTED] (Beschwerdegegnerin)

wegen Verletzung von Art. 5, 6 und 7 DSGVO wie folgt:

Die Beschwerde wird zurückgewiesen.

Rechtsgrundlagen: Art. 60 Abs. 8 DSGVO, Art. 20 Abs. 1 DSG, Art. 80 ff. LVG

Begründung:

A. Vorbringen der Parteien und Verfahrensgang

Der Beschwerdeführer reichte am 25. Mai 2018 eine Beschwerde bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn ein, die von dieser am 12. Juni 2018 an die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, Brandenburg als für den Beschwerdeführer zuständige Behörde gegründet auf den Wohnsitz des Beschwerdeführers weitergeleitet würde.

BO:

Beilage 1

Beschwerde des Beschwerdeführers, 25. Mai 2018

BO:

Beilage 2

E-Mail der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn,
12. Juni 2018

Als Fall mit grenzüberschreitender Datenverarbeitung wurde die Beschwerde seitens der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg am 10. Juli 2018 auf das IMI hochgeladen.

BO:

Beilage 3

IMI Case Entry von der Datenschutzbehörde Brandenburg, Case Nr. 45522, 10. Juli 2018

Die Beschwerdegegnerin hat ihre Hauptniederlassung in Liechtenstein. Gestützt auf Art. 56 Abs. 1 DSGVO hat die Datenschutzstelle Liechtenstein am 26. Juli 2018 akzeptiert, als federführende Datenschutzaufsichtsbehörde in diesem Fall tätig zu sein. Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg ist beteiligte Behörde gemäss Art. 60 Abs. 1 DSGVO.

BO:

Beilage 4

IMI Case Entry, Case Nr. 46432, von der DSS akzeptiert, 26. Juli 2018

Der Beschwerdeführer brachte in seiner Beschwerde vom 25. Mai 2018 die Verletzung von Art. 5, 6 und 7 DSGVO vor. Der Beschwerdeführer bringt vor, nie an dem von der Beschwerdegegnerin organisierten [REDACTED], „[REDACTED]“ zu haben. Als Beweis hierfür soll die Beschwerdegegnerin dem Beschwerdeführer einen Screenshot übermittelt haben. Der Beschwerdeführer bringt in der Beschwerde vor, dass die im Screenshot angeführte E-Mail-Adresse nicht seiner E-Mail-Adresse entspreche.

Mit Schreiben vom 7. August 2018 an den Beschwerdeführer wurden seitens der Datenschutzstelle als federführende Behörde zur weiteren Sachverhaltsabklärung verschiedene für das Verfahren erforderliche Dokumente und Bestätigungen beim Beschwerdeführer angefordert.

BO:Beilage 5

Schreiben der Datenschutzstelle an den Beschwerdeführer, 7. August 2018

Die Datenschutzstelle hat für die Übermittlung der angeforderten Dokumente und Informationen eine Frist von 14 Tagen ab Zustellung des Schreibens erteilt. Gemäss Rückschein ist das Schreiben am 13. August 2018 beim Beschwerdeführer eingegangen.

BO:Beilage 6

Übermittlungsbestätigung, Rückschein, 13. August 2018

Auf das genannte Schreiben hat der Beschwerdeführer innert der gesetzten Frist nicht reagiert. Zur Absicherung wurde per E-Mail mit Lesebestätigung vom 30. August 2018 beim Beschwerdeführer zurückgefragt, ob er zwischenzeitlich die angeforderten Dokumente und erbetenen zusätzlichen Informationen zu seinem Beschwerdefall an uns gesandt habe. Auch hierauf hat der Beschwerdeführer in keiner Weise reagiert.

BO:Beilage 7

E-Mail mit Lesebestätigung an den Beschwerdeführer, 30. August 2018

B. Rechtliche Beurteilung

Der Beschwerdeführer hat trotz Mängelbehebungsauftrag die angeforderten zusätzlichen Dokumente und Informationen, die für die rechtliche Beurteilung seiner Beschwerde erforderlich sind, nicht beigebracht.

Aufgrund fehlender Informationen sowie der die Beschwerde konkret stützenden Dokumente fehlt der Datenschutzstelle die Grundlage, die Beschwerde zur Verletzung von Art. 5, 6 und 7 DSGVO in datenschutzrechtlicher Hinsicht prüfen zu können und ist die Beschwerde zurückzuweisen. Ein diesbezüglicher Beschlussentwurf wurde am 21. September 2018 an die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg als beteiligte Behörde übersandt.

BO:Beilage 8

Beschlusseentwurf an die Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht Brandenburg, 21. September 2018

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg teilte am 11. Oktober 2018 über das IMI mit, mit dem Zurückweisungsbeschluss einverstanden zu sein.

BO:Beilage 9

IMI Bestätigung betr. Einverständnis zum Zurückweisungsbeschluss, 11. Oktober 2018

Es war daher spruchgemäß zu entscheiden.

Rechtsmittelbelehrung:

Gegen diese Verfügung kann binnen vier Wochen ab Zustellung Beschwerde bei der Beschwerdekommission für Verwaltungsangelegenheiten (Art. 20 Abs. 1 DSG) erhoben werden.

Die Beschwerde muss enthalten:

- Die Bezeichnung der angefochtenen Entscheidung;
- die Erklärung, ob die Entscheidung ihrem ganzen Inhalt nach oder nur in einzelnen Teilen angefochten wird, und in letzterem Fall die genaue Bezeichnung des angefochtenen Teils;
- die Beschwerdegründe;
- die Anträge;
- die Beweismittel, durch welche die Anfechtungsgründe gestützt und bewiesen werden wollen;
- die Unterschrift des Beschwerdeführers.

Gemäss Gesetz über die allgemeine Landesverwaltungspflege hemmen die Gerichtsferien den Lauf einer Rechtsmittelfrist. Der noch übrige Teil der Frist beginnt mit dem Ende der Gerichtsferien zu laufen. Die Gerichtsferien beginnen im Sommer jeweils am 15. Juli und dauern bis einschliesslich 25. August eines jeden Jahres.

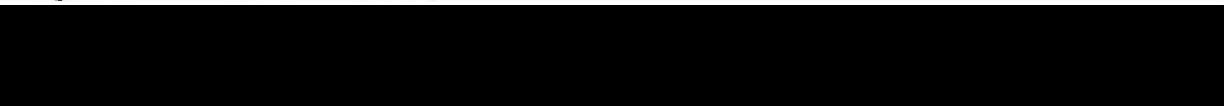
Vaduz, den 12. August 2019



Leiterin der Datenschutzstelle

Ergeht an (mit Zustellnachweis):

Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg,
Frau Dagmar Hartge, Stahnsdorfer Damm 77; DE-14532 Kleinmachnow (als beteiligte Behörde gemäss Art. 60 Abs. 7 DSGVO)



Beilagen: Beil. 1 bis 9 gemäss Beilagenverzeichnis

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	12 August 2019
LSA:	LI
CSAs:	DE-Brandenburg
Legal Reference:	Lawfulness of the processing (Article 6), Conditions for consent (Article 7), Principles relating to processing of personal data (Article 5)
Decision:	No violation
Key words:	Advertising, Lawfulness of the processing, Lack of evidence

Summary of the Decision

Origin of the case

The complainant alleged he had received unwanted advertising. After requesting access to his personal data, he received a screenshot from the controller showing the information he had allegedly shared in order to participate in an online competition. This included his address and contact details. The complainant argued that he had in fact not participated in the online competition and did not provide his consent, so he lodged a complaint assuming that a third party entered his contact details.

Findings

The LSA sent a request for further information to the complainant, which remained unanswered.

Decision

The case was rejected as no evidence was submitted by the complainant.



Summary of the Final Decision

Vaduz
August 27, 2019

Ref: 103.1.2/2019-283

IMI Case A60FD 75031

Decision of the Data Protection Authority of the Principality of Liechtenstein (DPA)

August 9, 2019

Parties:

Complainant: [may not be disclosed]

Controller: [REDACTED]

regarding a complaint lodged with the Data Protection Authority Liechtenstein

This complaint was treated as confidential. The decision has therefore been anonymised. The masculine form has been used throughout.

DECISION

The Data Protection Authority Liechtenstein finds

1. That [REDACTED] has contravened Art. 15 GDPR. Points 2, 4 and 5 of the information provided do not include all the necessary elements. In addition, the Data Protection Authority recommends that [REDACTED] specifies in Point 7 which supervisory authority is competent.
2. That the requests submitted by the legal representative are to be rejected.

1. Background to the case

On 18 November 2018 the complainant lodged a complaint against the controller for infringement of Art. 15 GDPR with the Commissioner for Data Protection of Lower Saxony.

In his complaint of 18 November 2018 the complainant alleges that he had requested the controller to provide full information pursuant to Art. 15 GDPR on 3 November 2018. The

complainant stated that the information provided by the controller pursuant to Art. 15 GDPR of November 2018 is deficient in the following points:

1. Point 2 (processing purpose) when compared with point 4 (recipients) of the controller's information under Art. 15 GDPR from November 2018 is incomplete resp. contradictory;
2. Point 5 (storage period) does not specify the specific storage period or the criteria according to which the storage period can be determined;
3. Point 7 (right of appeal) does not specify which authority shall be competent to handle complaints of the persons concerned.

As a cross-border case, the complaint was dealt with in accordance with Article 60 GDPR. The complaint was uploaded to IMI (IMI number 58561) on 24 January 2019. For [REDACTED] having its place of domicile in Liechtenstein the DPA Liechtenstein was the lead supervisory authority in accordance with Article 56 (1) GDPR.

The legal representative of the controller was requested by letter of 3 April 2019 to reply to the complaint by 17 April 2019. The legal representative replied to points 2, 5 and 7 of the controller's information under Art. 15 GDPR from November 2018 as follows:

1. Concerning point 2 (processing purpose) the legal representative of the controller stated that the complaint with respect to this point is incorrect since the marketing use of the personal data by third parties is no processing according to point 2. In the opinion of the legal representative of the controller only the controller's own processing shall be subject to point 2. Point 2 therefore shall not include that third parties store and use the data for their own purposes.
2. Concerning point 5 (storage period) the legal representative of the controller acknowledged in his counter-statement [REDACTED] even well-known companies such as [REDACTED] did not have more specific formulations with respect to the storage period there shall be no absolute necessity to name a specific storage period or the criteria for the storage period.
3. Concerning point 7 (right of appeal to the supervisory authority) the legal representative of the controller stated that the legal opinion quoted by the complainant to substantiate his complaint, namely the legal opinion found in Paal / Pauly / Paal, 2nd edition 2018, DS-GVO Art. 15 under point 29, is an individual opinion amongst many others. He stated that as of yet there is no evidence that the opinion quoted will become predominant. The legal representative of the controller further stated that there is no explicit obligation under Article 15 of the GDPR or from Recital 63 to designate the respective competent supervisory authority.

2. Complaint:

On the basis of the submissions of the complainant, the legal question was whether the controller gave incorrect and insufficient information to the complainant which the complainant had a right to receive according to Article 15 GDPR.

3. Legal framework:

a) Competence of the lead supervisory authority

[REDACTED] is a company domiciled in Liechtenstein, registered in the Liechtenstein Trade Register under number [REDACTED]. The GDPR has been in force since 20 July 2018 in Liechtenstein for all companies or other data processing authorities based in Liechtenstein. The complainant requested the controller on 3 November 2018 to provide full information pursuant to Art. 15 GDPR. The controller complied with this request for information beginning of November 2018. According to Art. 55 GDPR, the DPA Liechtenstein is the competent national data protection supervisory authority.

According to Art. 2 para. 1 GDPR, the GDPR applies to the full or partial automated processing of personal data. According to the definition in Art. 4 point 1 GDPR "Personal data" are all information relating to an identified or identifiable natural person, such as names, location data, online identification and other personal data as stated in Art. 4 point 1 GDPR. In accordance with the controller's letter of information from the beginning of November 2018 the complainant in particular processed the address data, contact details and date of birth. These data are personal data of natural persons in accordance with the legal definition of Article 4 (1) GDPR. According to Art. 2 para. 1 GDPR, the present complaint falls within the material scope of the GDPR.

b) Requests submitted by the processor's legal representative

As aforementioned, the legal representative of the controller raised several concerns regarding national administrative law. The DPA Liechtenstein rejected all these concerns.

c) Infringement of the right of access according to Art. 15 GDPR

c.1. Point 2 (processing purpose) and point 4 (recipient) of the controller's information under Art. 15 GDPR from November 2018 co states that they process personal data solely

[REDACTED] in accordance with the screenshot. On [REDACTED] and, the controller states in point 4 that they transfer the personal data to th [REDACTED] ccording to the screenshot for marketing purposes. The information given in p [REDACTED] s incomplete. In accordance with point 4, the transfer of personal data t [REDACTED] for marketing purposes should have been listed in point 2 as further processing of the personal data.

c.2. Point 5 (storage period) of the controller's information under Art. 15 GDPR from November 2018 merely states that the data are subject to the statutory retention periods. The indefinite specification of the retention periods in the context of the provision of

information is not sufficient. In accordance with the requirements of Art. 15 para. 1 letter d. GDPR the storage deadlines or the criteria for the determination of this duration in the provision of information must be specifically stated. It is not up to the person concerned to check which specific statutory retention periods apply to the processing of his personal data. The provision of information in point 5 is therefore incomplete.

c.3. Point 7 (right of appeal to the supervisory authority) of the controller's information under Art. 15 GDPR from November 2018 states that there is a right of appeal to a data protection supervisory authority. This corresponds to Art. 15 para. 1 letter f. GDPR. Art. 15 para. 1 letter f. GDPR does not specify with which data protection supervisory authority the complaint shall be filed. The legislator thus allows the complainant to decide with which data protection supervisory authority he intends to file his complaint. Some data protection experts (see for example Kühling / Buchner, General Data Protection Regulation, 2nd ed., 2018, p. 389 p. 39 in conjunction with p. 423 para) believe that the supervisory authority must in any case be specified with regard to the possibility of lodging a complaint. The DPA Liechtenstein does not fully agree with this opinion though. The DPA Liechtenstein considers that in principle the complainant is able to judge by himself which shall be the Data Protection Authority for filing his complaint. In accordance with the legislator's requirement under Article 12 (1) GDPR that the person responsible for data processing should facilitate the exercise of his rights in accordance with Articles 15 to 22 of the GDPR, the DPA Liechtenstein pronounces the recommendation, that the competent supervisory authority or at least the criteria for the designation of the supervisory authority shall be stated in the controllers' information pursuant to Art. 15 GDPR. However, there is no legal obligation to do so.

Summary Final Decision Art 60

Complaint

Compliance Order to Controller

Background information

Date of final decision:	27 August 2019
LSA:	LI
CSAs:	DE-Lower Saxony
Legal Reference:	Principles relating to processing of personal data (Article 5), Right of access (Article 15)
Decision:	Compliance order to controller
Key words:	Right of access, Information to data subjects

Summary of the Decision

Origin of the case

The complainant alleged that the controller infringed Article 15 GDPR by providing him with incomplete information concerning the purposes of the processing, the storage period and the right to appeal to a supervisory authority.

Findings

Concerning the processing purpose, the LSA found that the information provided by the controller was incomplete. In fact, it stated that personal data were processed solely for the purpose of participating in a prize competition. However, personal data were also transferred to sponsors for marketing purposes. The controller should have included this additional purpose of the processing when providing information to the data subject.

Concerning the storage period, the LSA found that the information provided by the controller was also incomplete. In particular, there was no specification on the storage period or the criteria according to which the storage period would be determined.

Concerning the right of appeal to a supervisory authority, the LSA found that the controller was under no legal obligation to specify which supervisory authority was competent. Nonetheless, the controller was advised to do so in order to facilitate the exercise of data subjects' rights.

Decision

The LSA found that the controller infringed Article 15 GDPR by not providing the complainant with correct and sufficient information regarding the purposes of the processing and the storage period of the data and therefore ordered compliance.

Summary Final Decision Art 60

Investigation

Imposition of a fine

Background information

Date of final decision: 16 May 2019

LSA: LT

CSAs: LV

Legal Reference: Principles relating to processing of personal data (Article 5), Lawfulness of processing (Article 6), Information to be provided where personal data have not been obtained from the data subject (Article 14), Responsibility of the controller (Article 24), Security of processing (Article 32), Notification of a personal data breach to the supervisory authority (Article 33), General conditions for imposing administrative fines (Article 83).

Decision: Imposition of fine

Key words: Data breach, unlawful processing, security of the processing

Summary of the Decision

Origin of the case

This case concerned the taking of screenshots by the data controller when a user made an online payment using its service. The user, however, was not notified about the screenshots being taken. The screenshots recorded personal data of the payer, such as their name and surname, numbers, recent transactions, loans, amounts, mortgages, etc. Moreover, the data controller had provided access to individuals that were not authorised for that purpose and did not report the relevant data breach.

Findings

Regarding the processing of personal data in screenshots: The LSA considered that the processing of the personal data by the controller was beyond what is necessary for the performance of the payment service, and was also stored for a longer period than necessary. The controller failed to demonstrate the need to collect such amount of personal data. Thus, the processing violates the

data minimisation and the storage limitation principles. Moreover, users are not informed of the processing. Therefore, the LSA considers that the processing of personal data is deemed as unlawful.

Regarding the publicity of the personal data: Due to a security breach, unauthorised individuals had access to the data concerned, since access could be gained on the controller's website merely by using the ID of the transaction number. The LSA found that the controller failed to implement the appropriate technical or organisational measures to ensure data security.

Regarding the notification of the personal data breach: The data controller failed to notify the relevant data breach as required by Art. 33 of the GDPR without providing a sufficient explanation of that failure to notify.

Decision

The LSA decided to impose a fine of 61.500 €(2,5% of the controller's total annual worldwide turnover).

Comments

This is the first fine issued by this SA under OSS mechanism.

Final decision

The Luxembourg supervisory authority (“CNPD”) refers to the complaint of [REDACTED] (hereinafter “[REDACTED]”) lodged with the supervisory authority of Spain.

The initial wording of the complaint on IMI stated that:

“The complaint is about a telegram sent by a third party to the complainant in which his full name and address are included, as well as an [REDACTED] order number. In this telegram the third party claims that he knows that a parcel purchased from [REDACTED] by him has been wrongly received by the complainant, and wants to get it back, threatening the claimant to go to the police. The third party access to the complainant personal data seems to indicate that his personal data have not been properly protected, thus the complaint.”

The complainant actually denies that the third party parcel was delivered to him, but after a first interaction with [REDACTED], [REDACTED] confirmed to him that according to his records, it was indeed delivered to his address. Further analysis made by the complainant with the courier seems to indicate that the courier messed up delivery references, as he received another parcel on that date, and they provided to [REDACTED] wrong delivery information which [REDACTED] linked to the order number of the third party.

[REDACTED] may have provided the personal data of the claimant to the user who requested the order, producing a violation of his privacy.”

Based on said complaint, the CNPD requested the controller (hereinafter [REDACTED]) to provide a detailed description of the issue relating to the processing of the complainant’s data as per Article 58.1(a) GDPR, in particular as regards the complainant’s personal data having allegedly been transmitted to a third party.

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has demonstrated that:

1. On 21 May 2018, [REDACTED] (a third party customer) purchased an item on [REDACTED] from [REDACTED], a [REDACTED] who delivers the products directly to its customers in Spain.
2. On 28 May 2018, [REDACTED] contacted [REDACTED] customer service indicating that he had previously contacted [REDACTED] – carrier in charge of delivery – to confirm the status of his order. In accordance with the facts reported by [REDACTED], when he provided the tracking number to [REDACTED], a [REDACTED] employee confirmed that this reference corresponded to a package that was going to be delivered to the complainant, and provided [REDACTED] with the full name and address of the complainant.

3. Given that [REDACTED] did not receive the package, he filed an [REDACTED]" claim on 29 May 2018 and after [REDACTED] investigated the case, it refunded the customer in full and suspended the selling privileges of the seller as a result of being in breach of [REDACTED] policies. [REDACTED] informed the CNPD that customers can request a refund via the [REDACTED] if they encounter a problem with items sold and fulfilled by a third party seller on [REDACTED]
4. As part of the internal investigation of [REDACTED], [REDACTED] contacted [REDACTED] on 17 October 2018 to check what delivery information they provide when someone calls and asks for delivery details via reference number. A [REDACTED] employee confirmed that the package in question had been delivered to the complainant on 28 May 2018, in line with the information [REDACTED] had previously provided to [REDACTED].
5. With respect to the correspondence between the complainant and [REDACTED], [REDACTED] has not found any account on [REDACTED] under the exact name or alleged address of the complainant, but only one under the name of XXX. Also, [REDACTED] stated that the account details do not show any communications linked to this account, nor a shipping address, payment information or any connection whatsoever with [REDACTED] order.
6. Therefore, it seems that in this instance, the company [REDACTED] provided the complainant's details to [REDACTED]. There is no further evidence that this information was provided by [REDACTED] to either [REDACTED] or [REDACTED] and it therefore seems that the data relating to the complainant must have already been stored by [REDACTED] in their systems and somehow connected by them to the order made by the customer [REDACTED].

The CNPD wants to point out that [REDACTED] provided all the necessary elements related to the complaint.

Thus, based on the above-mentioned explanations, the CNPD did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by [REDACTED].

As the complaint has only a limited personal impact, the CNPD has consulted the Spanish SA to determine whether the case could be dismissed. The CNPD and the Spanish SA agreed that, in view of the above, the data controller did not provide the seller with the complainant's address, that no further action is required and that the cross-border complaint (national reference [REDACTED]) should be closed.

A draft decision has been submitted by the CNPD on 3 April 2019 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number [REDACTED]).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Final decision

The Luxembourg supervisory authority (“CNPD”) refers to the complaint of [REDACTED] lodged with the supervisory authority of Spain.

The initial wording of the complaint on IMI stated that:

“The complainant states that he has received a parcel from someone unknown to him, and according to a receipt found with a watch inside the parcel, the sender is an [REDACTED] client that wanted to return the product [REDACTED] had just purchased. Apparently, [REDACTED] has given the complainant's name and address to a client, as a person who can receive and manage the devolution. He has contacted [REDACTED] by phone and by mail, but has got no answer to his request .”

Based on said complaint, the CNPD requested the controller (hereinafter [REDACTED]) to provide a detailed description of the issue relating to the processing of the complainant's data as per Article 58.1(a) GDPR, in particular as regards the lack of reaction by the controller to the complainant's request, as well as regards the complainant's personal data having allegedly been transmitted to a third party.

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has demonstrated that:

- A third party [REDACTED] purchased an item on [REDACTED] from XXX, [REDACTED] who delivers the products directly to its customers in Spain.
- [REDACTED] had also purchased a similar item from XXX, which [REDACTED] had delivered to him and therefore [REDACTED] had [REDACTED] shipping address. When the first customer sought to return the item to [REDACTED], the return label contained the address details of the complainant because [REDACTED] had included the complainant's address on the label for returns.
- According to [REDACTED], [REDACTED](XXX) behavior was a clear breach of [REDACTED] policies and after their own internal inquiry, [REDACTED] took corrective measures with this [REDACTED]
- [REDACTED] provided to the CNPD the answer given to [REDACTED], as well as the previous correspondence exchanged with [REDACTED]

Thus, based on the above-mentioned explanations, the CNPD did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by [REDACTED].

As the complaint has only a limited personal impact, the CNPD has consulted the Spanish SA to determine whether the case could be dismissed. The CNPD and the Spanish SA agreed that, in

view of the above, no further action is required and that the cross-border complaint (national reference [REDACTED]) should be closed.

A draft decision has been submitted by the CNPD on 3 April 2019 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number [REDACTED]).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	10 May 2019
LSA:	LU
CSAs:	CZ, DK, ES, FR
Legal Reference:	Lawfulness of the processing (Article 6), principles relating to the processing of personal data (Article 5), Security of processing (Article 32)
Decision:	No violation
Key words:	Lawfulness of the processing, Third party access to personal data, Rights of data subjects, Security of processing, e-commerce

Summary of the Decision

Origin of the case

The complainant states that they received a telegram sent by a third party in which their full name and address were included, as well as an order number. The third party claimed that a parcel purchased by him on the controller website had been sent to the complainant. The complainant states that their personal data may have been provided by the controller to the third party, thus violating the claimant's rights under GDPR.

Findings

Following an inquiry by the LSA, the controller has demonstrated that it was the courier who provided the complainant's details to the third party. The controller did not find any account on its website containing the personal details of the complainant, and there was no further evidence that the controller provided the personal data of the complainant either to the third party or to the courier. Therefore, it seems that the personal data relating to the complainant must have already been stored by the courier and got connected (by the courier) to the order made by the third party.

Decision

The LSA did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by the controller. The data controller did not provide the third party with the complainant's

personal details and therefore the cross-border complaint should be closed, since no further action is required.

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision: 10 May 2019

LSA: LU

CSAs: ES, FR, CZ

Legal Reference: Lawfulness of the processing (Article 6), Principles relating to the processing of personal data (Article 5), Right of access (Article 15), Security of processing (Article 32)

Decision: No violation

Key words: Lawfulness of processing, Third party access to personal data, Rights of data subjects, Right of access, Security of processing, e-commerce

Summary of the Decision

Origin of the case

The complainant received a parcel by an unknown person who wanted to return an item that she had purchased on the controller's website. The complainant's name and address had been indicated to the third individual as the place to return the parcel he had purchased.

Findings

The third-party was a customer of the controller that bought an item from a seller located in China, from which the complainant had also made a purchase. The personal data of the complainant had been disclosed to the third-party by the seller. After conducting an internal inquiry, the controller took corrective measures against the seller and informed the complainant.

Decision

The LSA found that there had been no violation of the GDPR. The LSA and the CSA agreed to close the cross-border complaint, since no further action is required.

Final decision

The Luxembourg supervisory authority (“CNPD”) refers to the complaint of [REDACTED] (hereinafter [REDACTED]) lodged with the supervisory authority of Austria.

The initial wording of the complaint on IMI stated that:

“The complainant tried to obtain the erasure of his [REDACTED] but the opponent didn't respond or reacted within a month.”

Based on said complaint, the CNPD requested the controller (hereinafter [REDACTED]) to provide a detailed description of the issue relating to the processing of the complainant's data as per Article 58.1(a) GDPR, in particular as regards the lack of reaction by the controller to the request to erasure within one month, as well as regards the closure of the complainant's account and the deletion of his personal data.

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has demonstrated that:

- The reason why [REDACTED] had not processed [REDACTED]'s request to close his [REDACTED] account connected to the e-mail address **XXX1** is because [REDACTED] contacted [REDACTED] each time from the e-mail address **XXX2**. This is not the e-mail address linked to the [REDACTED] account.
- [REDACTED] service agents contacted [REDACTED] informing him to contact them from the e-mail address connected to his [REDACTED] and if not possible to call their password hotline in order to change the login details to the [REDACTED] account. [REDACTED] also explained that this measure was necessary for security reasons as [REDACTED] wanted to prevent access from unauthorized third parties. [REDACTED] did not call the password hotline so that the authentication of [REDACTED] as the owner of the [REDACTED] account could not successfully be completed.

Following the receipt of the letter of the CNPD, [REDACTED] contacted [REDACTED] under his e-mail address **XXX1** asking him to reply to the e-mail if he wished to have the account connected to the e-mail address **XXX2** closed. This email was forwarded to the CNPD.

Thus, based on the above-mentioned explanations, the CNPD did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by [REDACTED]

As the complaint has only a limited personal impact, the CNPD has consulted the Austrian SA to determine whether the case could be dismissed. The Austrian SA informed the CNPD that the complainant had received the answer from [REDACTED] that he was satisfied with it and that the cross-border complaint (national reference [REDACTED]) should be closed.

A draft decision has been submitted by the CNPD on 3 April 2019 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number [REDACTED]).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	10 May 2019
LSA:	LU
CSAs:	AT, BE, CZ, DE - Mecklenburg-Western Pomerania, DE - Berlin, DE - Lower Saxony, DE - Bavaria (Private sector), DE - Saarland, DE - North Rhine-Westphalia, DK, FR, IT, NO, PL, SE, SI, SK
Legal Reference:	Right to Erasure (Article 17), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)
Decision:	No infringement of the right to erasure
Key words:	Right to erasure, e-commerce, Exercise of the rights of data subjects

Summary of the Decision

Origin of the case

The complainant requested the erasure of his customer account in the controller website, and he asserted that the controller did not respond within a month following his request.

Findings

The controller demonstrated that it did not delete the account because the request was lodged via a different email address than the one associated with the customer account. For security reasons, the controller contacted the complainant and asked him to submit the request from the same e-mail address associated with the customer account or, if not possible, to change his login details. The complainant did not take any action and therefore, the controller could not authenticate him as the owner of the customer account.

After receiving the letter from the LSA, the controller contacted the complainant on the e-mail address associated with the customer account and offered him to associate his other e-mail address to the customer account.

Decision

The LSA did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by the controller. The CSA to which the complaint was lodged informed the LSA that the complainant was satisfied with the answer from the controller and that the cross-border complaint should be closed.

Final decision

The Luxembourg Supervisory Authority (“CNPD”) refers to the complaint of [REDACTED] (hereinafter “[REDACTED]”) lodged with the supervisory authority of Spain.

The initial wording of the complaint on IMI stated that:

“The complainant has made a request of access to [REDACTED], but this company has not answered to this request. The reason for making the request is that his National Id number, his address and even his IP have been blocked by [REDACTED] therefore he is not able to create an user account in order to consume the services offered by this website. He wants to know the reason, so he asks for Access to all the data related to him in the [REDACTED] systems.”

Based on said complaint, the CNPD requested the controller (hereinafter [REDACTED]) to provide a detailed description of the issue relating to the processing of the complainant’s data as per Article 58.1(a) GDPR, in particular as regards the limitation of the complainant’s [REDACTED].

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has demonstrated that:

- [REDACTED]’s access request related to his status as a [REDACTED] [REDACTED] [REDACTED], which is a service owned and operated by [REDACTED] [REDACTED].
- As requested, [REDACTED] provided [REDACTED] with access to the data concerning him in that capacity related to his [REDACTED] account linked to the email address XXX, and a copy of the data. [REDACTED] also provided the CNPD with a copy of the communication sent to the complainant in response to his access request.

In addition, [REDACTED] has described the context regarding the rejections of [REDACTED]’s attempts to open a [REDACTED] account, so that the Supervisory authority/ies can gain a complete understanding of the rationale for the subject access request:

- On 31 January 2013, [REDACTED] opened a [REDACTED] account on [REDACTED]. This account was suspended on 27 November 2016 due to non-compliance with [REDACTED] [REDACTED] policies for [REDACTED] (the corresponding section of these policies is attached as **Document 2**), resulting in the [REDACTED]. As [REDACTED] indicated to [REDACTED] on 29 November 2016, he was required to appeal the decision and provide a valid plan of action in order to have the possibility to continue using [REDACTED] [REDACTED]. Following the suspension of his main account, [REDACTED] proceeded to open multiple new accounts to bypass the suspension [REDACTED], which contravenes [REDACTED] [REDACTED] policies (the corresponding section of these policies is attached as **Document 3**). When [REDACTED] identified this conduct, all other [REDACTED] accounts opened by [REDACTED] were closed in line with [REDACTED] policies from the end

of November 2016 to January 2017. As [REDACTED] tried to bypass [REDACTED] policy multiple times, [REDACTED] decided not to reinstate [REDACTED]'s main account, as well as the new accounts identified. Thus, as per [REDACTED] policies, [REDACTED] rejected [REDACTED]'s attempts to open a new [REDACTED] account.

In this case, [REDACTED] processed the complainant's information for fraud prevention purposes in accordance with its privacy policy. [REDACTED] nevertheless permitted the complainant to reopen a [REDACTED] account on 3 January 2019.

Thus, based on the above-mentioned explanations, the CNPD did not identify any infringement of the obligations set out in Regulation (EU) 2016/679 (GDPR) by [REDACTED].

As the complaint has only a limited personal impact, the CNPD has consulted the Spanish SA to determine whether the case could be dismissed. The CNPD and the Spanish SA agreed that, in view of the above, no further action is required and that the cross-border complaint (national reference 138660/2018) should be closed.

A draft decision has been submitted by the CNPD on 3 April 2019 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number [REDACTED]).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision: 10 May 2019

LSA: LU

CSAs: AT, BE, CY, CZ, DE - Berlin, DE - Lower Saxony, DE - Rhineland-Palatinate, DE - Bavaria (Private sector), DE - Mecklenburg-Western Pomerania, DK, ES, FI, FR, IE, IT, PL, SE, SK, NO

Legal Reference: Right of access by the data subject (Article 15), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)

Decision: No infringement

Key words: Right of access, exercise of the rights of the data subject, e-commerce

Summary of the Decision

Origin of the case

The complainant requested access to his personal data held by the controller because his national ID number, his address and his IP had been blocked by the controller's platform and he was thus unable to use its services. He wanted to know the reason and thus requested access to his data.

Findings

The controller demonstrated that it had provided the complainant with access to the data concerning him and his seller account. The controller provided the relevant communication to the LSA and it also clarified that the blockage of the complainant's information was due to a violation of the controller's selling policies. The controller also explained that it had granted the complainant the right to appeal the blockage, but instead he tried to circumvent the decision by opening new seller accounts, which were blocked. However, the controller allowed him to create a customer account.

Decision

The LSA found that there had been no violation of the GDPR, since the controller had granted the complainant the right to access to his data. The LSA and the CSA agreed to close the cross-border complaint, since no further action is required.

Final decision

The Luxembourg supervisory authority (“CNPD”) refers to the complaint of Mr [REDACTED] (hereinafter “[REDACTED]”) lodged with the supervisory authority of Spain.

The initial wording of the complaint on IMI stated that:

“The complainant states that his data has been inscribed in the insolvency file ASNEF associated to a debt which has not been notified. The date of the entry is [REDACTED] and the creditor who ordered the inscription is [REDACTED]. The debt amounts to [REDACTED]”

Based on said complaint, the CNPD requested the controller (hereinafter “[REDACTED]”) to provide a response to the issue raised as per Article 58.1(a) GDPR, in particular as regards to the lawfulness of the processing of the complainant’s personal data.

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has provided all necessary documentation, including general explanations on the management and administration of credits owned by third parties as well as specific explanations related to the complainant’s personal situation. The documentation was provided both in English and in Spanish.

Thus, based on this documentation, the CNPD is satisfied that [REDACTED] fulfilled its obligations under Regulation (EU) 2016/679 (GDPR) by immediately addressing the issue.

As the complaint has only a limited personal impact, the CNPD has consulted the Spanish SA to determine whether the case could be dismissed. The CNPD and the Spanish SA agreed that, in view of the above, no further action is required and that the cross-border complaint (national reference E/08073/2018) could be closed.

A draft decision has been submitted by the CNPD on 7 February 2020 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 108026).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Summary Final Decision Art 60

Complaint

Dismissal of the case

EDPBI:LU:OSS:D:2020:92

Background information

Date of final decision:	10 March
LSA:	LU
CSAs:	ES
Legal Reference:	Lawfulness of processing (Article 6)
Decision:	Dismissal of the case
Key words:	Lawfulness of processing, Legal basis, Credit management, Credit administration

Summary of the Decision

Origin of the case

The complainant stated that their data had been inscribed in the insolvency file “ASNEF” upon request of the controller. Their file was associated to a debt that had not been notified to them.

Findings

The LSA requested the controller to provide a response to the complainant, especially with regards to the lawfulness of the processing of the complainant’s personal data.

The controller timely submitted the requested information, including general explanations on the management and administration of credits owned by third parties as well as specific explanations related to the complainant’s personal situation.

Decision

The LSA was satisfied that the controller fulfilled its obligations under the GDPR by immediately addressing the issue.

Final decision

The Luxembourg Supervisory Authority (“CNPD”) refers to the complaint of [REDACTED] (hereinafter “[REDACTED”)) lodged with the supervisory authority of Austria.

The initial wording of the complaint on IMI stated that:

“The complainant has terminated his contract with [REDACTED] [REDACTED] is a trademark of the controller). He wanted to assert his right to erasure, but his data is still available on the web portal. the Controller didn't answer his request within a month.”

Based on said complaint, the CNPD requested the controller [REDACTED] (hereinafter “[REDACTED”)) to provide a response to the issue raised as per Article 58.1(a) GDPR, in particular as regards the complainants right to erasure.

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has demonstrated that all the complainant’s data have been erased, except from the transaction data, which must be kept ten years according to article 16 of the Luxembourg commercial code.

Thus, based on the above-mentioned explanations, the CNPD is satisfied that [REDACTED] has fulfilled its obligations under Regulation (EU) 2016/679 (GDPR) by immediately addressing the issue.

As the complaint has only a limited personal impact, the CNPD has consulted the Austrian SA to determine whether the case could be dismissed. The CNPD and the Austrian SA agreed that, in view of the above, no further action is required and that the cross-border complaint (national reference D130.070) could be closed.

A draft decision has been submitted by the CNPD on 7 February 2020 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 107959).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Summary Final Decision Art 60

Complaint

Dismissal of the case

EDPBI:LU:OSS:D:2020:91

Background information

Date of broadcast:	10 March 2020
LSA:	LU
CSAs:	AT, DE, SK
Legal Reference:	Right to erasure (Article 17), Right to restriction of processing (Article 18), Powers (Article 58)
Decision:	Dismissal of the case
Key words:	Right to erasure

Summary of the Decision

Origin of the case

The complainant terminated his contract with the controller. Following termination, his data was still available on the web portal. The controller failed to respond to the erasure request within a month.

Findings

The LSA received the requested information within the set timeframe. Furthermore, the controller was able to demonstrate that the complainant's data had been erased. This did not include transaction data which must be kept for a period of ten years under Article 16 of the Luxembourg Commercial Code.

The LSA was satisfied that the controller had fulfilled its obligations under the GDPR by immediately addressing the issue.

Decision

Both the LSA and CSA agreed that no further action was required and that the case could be closed.

Final decision

The Luxembourg Supervisory Authority (“CNPD”) refers to the complaint of [REDACTED] (hereinafter “[REDACTED]”) lodged with the supervisory authority of Germany, Rhineland-Palatinate.

The initial wording of the complaint on IMI stated that:

“The complainant had entered a contract for a credit card with the controller, but he did not accept the release from banking secrecy in the terms of service. Since the controller has insisted on this clause, the complainant withdrew from the contract. He now mainly wishes his data to be erased.”

Based on said complaint, the CNPD requested the controller [REDACTED] (hereinafter “[REDACTED”]) to provide a response to the issue raised as per Article 58.1(a) GDPR, in particular as regards the complainants right to erasure.

The CNPD received the requested information within the set timeframe.

Following an enquiry by the CNPD, [REDACTED] has demonstrated that the complainant was provided with all the requested information and that the contract was indeed terminated. The controller also demonstrated that the complainant’s data has been erased, except from the transaction data, which must be kept ten years according to article 16 of the Luxembourg commercial code.

Thus, based on the above-mentioned explanations, the CNPD is satisfied that [REDACTED] has fulfilled its obligations under Regulation (EU) 2016/679 (GDPR) by immediately addressing the issue.

As the complaint has only a limited personal impact, the CNPD has consulted the supervisory authority of Germany, Rhineland-Palatinate to determine whether the case could be dismissed. The CNPD and the supervisory authority of Germany, Rhineland-Palatinate agreed that, in view of the above, no further action is required and that the cross-border complaint (national reference 4.02.18.525) could be closed.

A draft decision has been submitted by the CNPD on 7 February 2020 to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 107971).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission

Summary Final Decision Art 60

Complaint

Dismissal of the case

EDPBI:LU:OSS:D:2020:92

Background information

Date of final decision: 10 March 2020

LSA: LU

CSAs: DE-RP, FR

Legal Reference: Article 17 (Right to erasure ('right to be forgotten'))

Decision: Dismissal of the case

Key words: Right to erasure, Deletion, Data retention

Summary of the Decision

Origin of the case

The complainant had entered into a contract for a credit card with the controller, but as the complainant did not agree with the controller's terms of service, the complainant withdrew from the contract and asked the controller to erase their data.

Findings

Following an enquiry by the LSA, the controller demonstrated that the complainant's data had been erased, except from the transaction data, which must be kept for ten years according to Article 16 of the Luxembourg Commercial Code.

Decision

The LSA was satisfied that the controller had fulfilled its obligations under the GDPR by immediately addressing the issue and decided to close the case.

FINAL DECISION



Datu valsts inspekcija

Blauma a iela 11/13-15, R ga, LV-1011, t lr. 67223131, fakss 67223556, e-pasts info@dvi.gov.lv, www.dvi.gov.lv



Decision

in Riga

December 3, 2019

No. 2-2.2/52

Re: imposing an obligation

Data State Inspectorate of the Republic of Latvia (hereinafter - the Inspectorate) carried out an inspection of data processing by SIA [REDACTED] No. [REDACTED] (hereinafter SIA) based on a complaint from applicant [REDACTED] (hereinafter the Applicant), dated 21 January 2019 (hereinafter - the Complaint) transmitted by the Republic of Ireland and the consistency mechanism set out in Article 63 of the General Data Protection Regulation¹ (hereinafter - the GDPR).

The Inspectorate finds that the Complaint and the information in the attachment shows that on January 20, 2019 the Applicant contacted SIA by e-mail. The Applicant informed SIA about the erroneous registration on the SIAs website [REDACTED] and requested the removal of two registered profiles named [REDACTED] and [REDACTED] of Applicant. The Inspectorate finds that SIA, by e-mail dated January 21, 2019, provided the Applicant with a reply informing the Applicant that SIA could not comply with the Applicant's erasure request.

As part of the inspection, the Inspectorate requested and received information on 6 June 2019 from SIA (registered with the Inspectorate under No. 2-4.3/914-S). The Inspectorate notes that SIA, in its response letter dated June 4, 2019 (the Response Letter), inter alia, stated that "*We have blacklisted the email address [REDACTED], so no e-mail will be sent to us*".

Within its competence, the Inspectorate shall determine and indicate the following in the assessment of the above case.

According to Article 1 (2) of the GDPR, This Regulation protects fundamental rights and freedoms of natural persons and in particular - their right to the protection of personal data.

Article 2 (1) determines that This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

According to Article 4 (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'), however according to Article 4 (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. It follows that an e-mail address, if it contains a person's name and surname, is to be considered as personal data and any processing of such data, including their blacklisting, constitutes processing of personal data within the meaning of the GDPR.

Pursuant to Article 4 (7) of the GDPR, the controller is responsible for the compliance of the processing of personal data with the Regulation, namely a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of processing. In this case, SIA is responsible for personal data processing of the Applicant.

The Inspectorate indicates that processing of personal data must be carried out in accordance with the GDPR, including Article 6, which provides that the processing of personal data shall be lawful only if and to the extent that at least one of the legal grounds referred to in Article 6 (1) applies, namely, consent, performance of contract, legal obligation, public interest, protection of vital interests and respect for legitimate interests. In addition to providing the legal basis, the controller must also comply with other conditions laid down in the GDPR, such as Article 5 (1) (a) of the GDPR stipulating that the processing shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. However, Article 5 (1) (b) of the GDPR states that data shall be collected for specified, explicit and legitimate purposes. If these conditions are not met, the processing of personal data shall be incompatible with the GDPR and shall not happen.

Furthermore, in accordance with the principle of accountability set out in Article 5 (2) of the GDPR, it is the controller who has the responsibility to ensure that the personal data processing process which shows that the processing of personal data complies with data protection regulatory framework requirements.

In addition, pursuant to Article 24 (1) and (2) of the GDPR, the controller shall take appropriate technical and organizational measures to take account of the nature, extent, context and purposes of the processing and the various degrees of probability and severity of the rights and freedoms of natural persons. ensure and be able to demonstrate that the processing is in accordance with the GDPR. Thus, it is understandable that the controller provides the technical and organizational means to secure data processing.

Article 25 (1) of the GDPR determines that taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Thus, it is understandable that the Controller provides the technical and organizational means to secure data processing.

Article 15 – Article of the GDPR 22 sets out the data subject's rights, which states that the data subject is entitled to request in writing the information set out in this Article related to the data subject's personal data.

Article 17 of the GDPR provides that the data subject has the right to request the erasure of his or her personal data. Article 17(1) and (2) of the GDPR lays down the right to “be forgotten”. In accordance with Article 17(1) of the GDPR, data subject has the right to obtain that the controller delete the personal data of data subject without undue delay, and the controller is obliged to delete personal data without undue delay if one of the conditions referred to in paragraphs 1 and 2 of this Article exists. It follows that the controller is obliged to respond to the data subject's request and delete the personal data of the data subject if any of the conditions set out in Article 17 (1) and (17) of the GDPR are met.

The Inspectorate evaluation of the complaint the information relating to the Applicant's personal data, concludes the following. Conditions of Article 17 (1) of the Regulation have been met and the data subject (Applicant) has withdrawn his consent to the processing of personal data on the basis, of which the SIA processed the personal data of the Applicant.

The Inspectorate, having assessed the information contained in the Response Letter to SIA, concludes that SIA is still processing the Applicant's personal data because the LLC has blacklisted the Applicant's personal data (email address [REDACTED]).

Having assessed the response provided by SIA, the Inspectorate concludes that there is no legal basis for SIA to continue processing and storing the Applicant's personal data (e-mail address [REDACTED]) in the SIA blacklist.

Article 31 of the GDPR states that the controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

Article 58 (2) of the GDPR provides that the Inspectorate, as each supervisory authority for the processing of personal data, has several corrective powers. Article 58 (2) (g) of the GDPR states that the Inspectorate shall have the power to order the rectification or erasure of personal data or to restriction of processing pursuant to Articles 16, 17 and 18 and to inform the recipients the data have been disclosed pursuant to Articles 17 (2) and 19.

Article 66 (1) of Administrative Procedure Law determines that in considering the usefulness of the issue of, or of the content of an administrative act (Section 65), an institution shall take a decision regarding: 1) the necessity of the administrative act for the attaining of a legal (legitimate) goal; 2) the suitability of the administrative act for the attaining of the relevant goal; 3) the need for the administrative act, that is, whether it is possible to attain such goal by means which are less restrictive of the rights and legal interests of participants in the administrative proceeding; and 4) the conformity of the administrative act, comparing the infringement of the rights of a private person and the benefits for the public interest, as well as taking into account that substantial restriction of the rights of a private person may only be justified by a significant benefit to the public.

Having assessed the information provided in this administrative act, the Inspectorate concludes that the detected infringement in the field of data protection of natural persons is continued, therefore, only the issuance of an administrative act can increase the SIA's awareness of its noncompliance with the GDPR and prevent repeated infringements. The administrative act is issued for the purpose of protecting the Applicant's rights to the protection of his personal data established in the Satversme (the Constitution). The Inspectorate finds that the relevant objective of this Decision cannot be achieved by less restrictive means of the SIA. There is no legal basis for SIA to process the Applicant's email address on the blacklist of SIA.

By this administrative act, the rights of the SIA as a private person are minimally infringed, while it is in the public interest to obtain assurance on the effective protection of personal data by the Inspectorate. In this administrative act, an infringement of the rights of the company as a private righholder is proportional to the benefit of the public interest, the latter exceeding the first.

In view of the above and on the basis of Article 58 (2) (g) of the GDPR, Article 23 of the Personal Data Processing Act (hereinafter - FPDAL), Article 63 (1)(2) of the Administrative Procedure Law (hereinafter – APL), ***the Inspectorate shall decide:***

1. ***Impose an obligation to the SIA to delete the Applicant's personal data immediately, but not later than 20 December 2019 - the e-mail address [REDACTED] from the blacklist of SIA, as well as other possible storage sites, if data processing is carried out wholly or partly by automated means, or the Applicant's personal data are processed in a filing system or are intended to form part of a filing system where the processing is not carried out by automated means.***
2. ***The future activities of SIA shall comply with the requirements of the GDPR and other laws and regulations referred to in this Decision. SIA shall assess the different degrees of likelihood and severity of risks to the rights and freedoms of natural persons, taking into account the nature, extent, context, purposes and technical and organizational measures taken to protect personal data and prevent their possible unlawful processing. SIA shall provide a mechanism to prevent such situations from occurring in the future of SIA and prevent any inconsistencies, if any, by ensuring the legal processing and protection of personal data.***

Please inform the Inspectorate in writing of the execution of the order by **20 December 2019** (*last day for submitting a written reply to the mail or for sending electronically with a secure electronic signature*).

This decision is an administrative act within the meaning of the APL and will be notified to the SIA by post as a recorded mailing. Article 70 (1) of the APL determines that, provided that it is not otherwise stipulated in an external regulatory enactment or the administrative act itself, an administrative act shall come into effect at the time the addressee is notified of it. In accordance with Article 70 (2) of the APL and Article 8 (3) of the Law on Notification, A document which has been notified as a registered postal item shall be deemed notified on the seventh day after handing it over to the post office.

In accordance with Article 24(2) of the FPDAL, Article 70, Article 76(2) and Article 79(1) of the APL, this decision may be appealed to a court in accordance with the requirements laid down in Article 188 (2) and Article 189(1), Article 29(3) of the Law On Judicial Power and according to Decision No 307 of the Board of Justice of 5 March 2018 on Courts, Territories and Locations of their Activities - within one month from the date of their entry into force at the relevant courthouse of the Administrative District Court, at the location of the registered office of the Company.

Acting Director

/signature/



Summary Final Decision Art 60

Complaint

Compliance order

Background information

Date of final decision:	3 December 2019
LSA:	LV
CSAs:	DE-Berlin, DE-Hesse, DE-Rhineland-Palatinate, DK, FR, IE, IT, PL, NO
Legal Reference:	Lawfulness of processing (Article 6), Right to erasure (Article 17), Right to be informed (Article 15)
Decision:	Infringement of the GDPR, Order to comply
Key words:	Right to erasure, Right to be informed, Blacklisted email

Summary of the Decision

Origin of the case

The complainant alleged that their request for deletion of their personal data had not been complied with.

Findings

After an investigation, the LSA found that after accidentally signing up to the controller's services, the complainant had contacted the controller to ask for the deletion of two accounts made in his name. The controller responded the next day that this would not be possible. The controller also blacklisted the complainant's email address, thereby blocking reception of its emails.

Decision

The LSA found that the controller did not have a legal basis to continue processing and storing the complainant's personal data on a blacklist. An administrative act was issued by the LSA, with the order for the controller to delete the complainant's personal data from the blacklist or from any storage site or filling system by 20 December 2019. In addition, the controller was given an order to assess the degree of risk to the rights and freedoms of natural persons, taking into account the nature, extent, context, purposes and technical and organizational measures taken to protect personal data and prevent their possible unlawful processing was issued, and to provide a mechanism to prevent such

situations from happening in the future. The controller was asked to inform the LSA of the execution of the order by 20 December 2019.

/Coat of arms of Republic of Latvia/
Data State Directorate

Blauma iela 11/13-15, Riga, LV-1011, telephone 67223131, fax 67223556, e-mail info@dvi.gov.lv, www.dvi.gov.lv

Case No.L-2-4.3/4627

Decision

Riga,
8 November 2019

No.2-2.2/45

On imposition of administrative penalty

1. Institution (official) adopting the decision: [REDACTED] (hereinafter—the Official), the Head of Personal Data Processing Supervision Department of the Data State Inspectorate (hereinafter—the DSI) in accordance with the DSI order No.1-2.1/120 of 28.11.2018 “On examination of the administrative infringement case”, Article 58(2)(i) of the General Data Protection Regulation¹ (hereinafter—the GDPR), Section 5(1)(2) of the Personal Data Processing Law (hereinafter—the PDPL) and Section 236.¹⁰ of the Latvian Administrative Violations Code (hereinafter—the LAPC).

2. Case examination date: 08.11.2019

3. Data about the person the case applies to: Limited Liability Company [REDACTED], registration number [REDACTED] (hereinafter—SIA).

SIA representative did not appear at the case examination. The official finds that on 08.11.2019, the DSI received an e-mail of 07.11.2019 supposedly from the representative of SIA [REDACTED] (DSI, 08.11.2019, reg. No.2-4.3/1854-S) with the information and requests made in it. The letter did not contain a request to postpone the case examination.

In accordance with Section 4(1) and (2) of the Law On Legal Force of Documents, in order for a document to have legal force the name of the authors of the document, the date of the document and the signature shall be included. The document having no legal force is not binding on other organisations and natural persons, yet it is binding on the author of the document.

The Official finds that the Letter is not signed in person, as well as is not signed with a secure electronic signature. Therefore, the letter has no legal force and the DSI is not bound by it.

In light of the foregoing, the Official recognises that no conditions have been stated, which would be the basis for the postponement of case examination, it is therefore possible to examine the case without participation of the person called to administrative liability.

4. Summary of circumstances identified in case examination:

4.1. The Official finds that administrative infringement case files (hereinafter—Case Files) contain a complaint of [REDACTED] of 22.08.2018 with an annex transferred by the Spanish data protection authority (hereinafter—the Complaint).

The DSI finds that it follows from the Complaint and the information available in the annex that on 10.07.2018, [REDACTED], the citizen of the Kingdom of Spain, purchased [REDACTED]

¹ Regulation 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 (the General Data Protection Regulation)

for EUR 44.00 in online store [REDACTED], which is confirmed by invoice No [REDACTED] (hereinafter—the Invoice). It follows from the Complaint that in order to receive the product, [REDACTED] placed an order of the product on [REDACTED] and transferred his personal data, namely, name, surname and mobile phone number. In his Complaint, [REDACTED] refers to the GDPR, Chapter III, “Rights of the data subject”, which provides that where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all information on the contact details of the controller or the data protection officer, the purpose of the use of the personal data, the category of the personal data collected by the company, the legal basis for the processing of the personal data, the period for which the personal data will be stored, the third party to which the personal data are disclosed, if the personal data are transferred to a foreign recipient within the EU, the rights of the personal data subject. It follows from the Complaint that [REDACTED] prior to completing the order form on [REDACTED] was deprived of the opportunity to read the above-mentioned information and at the same time [REDACTED] has a section called Privacy Policy², where the information provided does not meet the GDPR requirements.

The Official finds that the annex to the Complaint contains an Invoice issued to [REDACTED] for the sale of [REDACTED]. According to the Invoice, [REDACTED] is specified as the seller, but [REDACTED], is indicated as the address of the seller of the goods. (DSI 02.01.2019 reg. with No.1-5.2/149-S)

The Official finds that in light of the foregoing, based on the consistency mechanism referred to in Article 63 of the GDPR, the DSI opened an investigation regarding the personal data processing referred to in the Complaint.

4.2. The Official finds that the Case Files contains the DSI statement of 10.01.2019 with annex No.7-5.1/1. It follows from the information included in the statement and the annex that DSI officials, having collected the publicly available information about [REDACTED], learned that [REDACTED] is a food supplement registered in the Register of Food Supplements of the Food and Veterinary Service of the Republic of Latvia under No. [REDACTED] and this product was produced in the EU at the commission of SIA. (hereinafter—Statement No.1)

4.3. The Official finds that the Case Files contain information from the Register of Enterprises on Lursoft that SIA is registered at [REDACTED]. In accordance with the information from the register, the type of activity of SIA is retail sale via mail order or via Internet.

4.4. The Official finds that the Case Files contain a statement of DSI of 25.01.2019 with annex No.2-5.1/19. It follows from the information included in the statement and the annex that DSI officials checked the websites [REDACTED] and [REDACTED] and it has been stated that the information available on the websites provides evidence of distribution of [REDACTED]. The visual examination has revealed that the websites have an electronic order window. Persons should specify their name and phone number when submitting an order. These websites have a similar layout and the type of use. These websites contain privacy policies having the same content and location and the privacy policy of [REDACTED] corresponds to the one indicated in the Complaint of [REDACTED]. The reference to [REDACTED] appears at the bottom of each website.

The examination has also revealed that [REDACTED] offers an opportunity to select a country, for example, Germany, Portugal, Czech Republic, Lithuania, Poland and other, as a result, depending on the selected country, the websites offer information about [REDACTED] in the language of the selected country without changing the visual layout of the website. The reference to [REDACTED] appears at the bottom of each website. (hereinafter—Statement No.2).

² [REDACTED]

4.5. The Official finds that the Case Files contain the reply letter No.02/2019 of SIA of 22.03.2019 to the DSI's request on the data processing performed by SIA, where SIA, inter alia, explained that [...] *SIA performs its activity in the following form: An agreement has been concluded with an advertising company on placement of advertisements of goods in mass media. A proper agreement has been concluded with a call centre, employees of which receive and process calls from potential customers based on the advertising information. Information and needs of customers are transferred to the warehouse of SIA, which processes orders. The delivery of the goods takes place using a courier service, with which a respective cooperation agreement has been concluded.* [...]

All cooperation agreements and processes will be reviewed during the audit in the nearest time. When the audit is over, under a contract, an action plan will be developed, processes and internal regulations will be introduced ensuring the fulfilment of the requirements for personal data protection in accordance with the requirements of Regulation". (DSI 26.03.2019 reg. under No.2-4.3/483-S) (hereinafter—Explanation No.1).

4.6. The Official finds that the Case Files contain the reply letter of SIA of 17.05.2019 to the DSI's request on the data processing performed by SIA, where SIA explained that [...] *Personal data collection, recording, organisation, storage, consultation, use, disclosure and erasure (destruction) is carried out by SIA in accordance with Article 4(2) of the GDPR.*

SIA has the following personal data about customer: name, surname, telephone, delivery address.

In accordance with Article 6 of the GDPR, the legal basis for collection, recording, consultation, use of personal data processed by SIA, when sending, is fulfilment of remotely concluded agreements towards the data subject on the basis of a cooperation agreement of SIA with the customer attraction company (call centre) (pursuant to Article 6(1)(b) of the GDPR), the party to which the data subject is. Furthermore, storage and erasure of respective data takes place in accordance with the record-keeping and archiving requirements set in the country, as well as the fulfilment of accounting, which are in accordance with Article 6(f) of the Regulation.

The purpose of each processing of data by SIA is the fulfilment of legal regulations and assumed contractual liabilities towards the data subject by delivering the ordered goods.

Taking into account that the collection of personal data takes place through mediation to fulfil the distance agreement concluded with the data subject and the fact that the data are obtained by the company, with which SIA has concluded an agreement (call centre), then the respective service providers (call centres) inform customers of SIA on the performed personal data processing and the conditions defined in Article 14(5)(a) and (b) of the GDPR are applied when the company obtains personal data.

In addition, SIA explained that currently it is being subject to reorganisation and a proper personal data processing policy is being developed, as a result of which the information will be published upon completion of this process. [...] In any case, if the data subject would submit a request fulfilled in accordance with the requirements of Article 15 of the GDPR, then SIA would kindly provide a proper reply.

With regard to [REDACTED] SIA explained that [...] [REDACTED] is an advertising web page about the product of SIA developed on the instruction of SIA based on a contract, where it is possible to order a call-back from the customer centre (call centre) of the cooperation partner of SIA, which also receive data entered there using certain organisational and technical solutions at any time. (DSI 20.05.2019 reg. No.2-4.3/791-S) (hereinafter—Explanation No.2)

4.7. The Official finds that the Case Files contain the DSI statement of 29.05.2019 with annex No.2-5.1/116. It follows from the information included in the statement and the annex that the DSI officials visually inspected the website [REDACTED] and this website contained information about [REDACTED] and an electronic order window for persons. Persons should specify their name and phone number when submitting an order. Clicking on the Privacy Policy window

at the bottom of the website, information on protection of personal data is available. This information is identical to the one indicated in the Complaint, namely, the one posted on [REDACTED]. When clicking on the Report window at the bottom of the website, it has been stated that the website contains a communication tool, where a text message can be left (for example, feedback can be provided or a question can be asked indicating the person's name and/or surname, phone number and e-mail. The reference to [REDACTED] appears at the bottom of the website. (hereinafter—Statement No.3)

4.8. The Official finds that the Case Files contain reply letter of SIA of 21.06.2019 to the DSI's request on the data processing performed by SIA, where SIA explained that [...] *SIA cannot answer the question regarding the information about [REDACTED]*, on [REDACTED], because *SIA was not the developer of that website. SIA concluded an agreement with [REDACTED] on the development of this website, on provision and development of advertising of products produced by SIA, in this case [REDACTED], which provided that [REDACTED] was entitled to involve third parties for such activities. SIA assumes that [REDACTED] in that case involved [REDACTED] as a third party for the development of advertising and software. [...]*

The annex contains the Agreement No. [REDACTED] concluded between SIA and [REDACTED] on provision of marketing services. The agreement states that [REDACTED] provides SIA with advertising services, which under this agreement are the services that ensure posting of materials raising public awareness of SIA on the internet on its websites, which are selected by SIA (Sub-Clauses 1.1 and 1.2 of the Agreement). The advertising and information module is static (with a static image) or animated, graphic information block and/or information block containing text of any form and layout (section—general designations). The agreement does not contain conditions for the processing of personal data.

SIA explained that [...] *The information entered on the website and data entered on it (country, phone No. and name) are operated by SIA product distributors and providers of marketing services, with whom SIA has concluded agreement. Therefore, data entered on the website are processed by [REDACTED] and [REDACTED] (hereinafter—marketing companies), who further perform processing and use of these data for marketing and product distribution purposes. Only when the marketing companies have concluded a distance agreement with the customer and obtained necessary data from the data subject on contact information for sending the product (name, surname, address, phone No.), information on the need to deliver the product is transferred to SIA in accordance with concluded agreements [...].*

The annex contains Agreement No. [REDACTED] and Agreement No. [REDACTED] on provision of telemarketing services, which were concluded between SIA and [REDACTED] and SIA and [REDACTED] respectively. Sub-Clause 1.1 (Subject matter of the Agreement) of both agreements provides that the companies undertake to provide telemarketing services (services related to distribution of SIA goods using phone communication services), while SIA undertakes to accept provided services and pay for them properly. When selling products, the operator should use proper conversation scenarios issued by SIA. Each conversation scenario is considered an annex to this agreement and its integral part. Whereas Clause 5 of both agreements lays down confidentiality obligations, inter alia, Sub-Clause 5.4 provides that information received by the operators as part of provision of the service, shall be deemed confidential and property of SIA. Transfer of information (all or partial) to third parties without written consent of SIA shall be prohibited (a fine of EUR 5000 is set for the infringement). The content of the agreement corresponds to the agreement concluded between the controller and the processor.

SIA explained that [...] *For the purpose of fulfilment of the product delivery agreement personal data are entered and processed by marketing companies, which are entered by*

representatives of marketing companies (operators) in software of SIA. SIA has the following data on purchasers of products (concluded distance agreements): name, surname, delivery address and phone No., no other data about customers of SIA are obtained from marketing companies. SIA does not process e-mails of data subjects. SIA is the controller of the above-mentioned personal data processing. SIA has not ensured observation of the transparency and accountability principle until now, because SIA is undergoing restructuring and these activities were postponed due to shortage of resources, including measures for evaluation of data processing. SIA does not ensure provision of information to the data subject, when receiving data or delivering a parcel, considering the fact that the information on data obtained and reasons of their processing are already known to the data subject and this information is not used for other purposes. The personal data available to SIA are stored only electronically in [REDACTED], Customer Relationship Management software, and in the Accounting programme. The obtained data are stored in accordance with Article 6(1)(b) and (c) of the GDPR, namely, for the performance of a contract and for compliance with the duty to provide evidence of a transaction for accounting purposes. In addition, the duties defined in Section 41 of the Cabinet Regulation No.585 "Regulations on Keeping and Organisation of Accounting" of 21 October 2003 and Sections 2 and 7 of the Law "On Accounting" are carried out. SIA transfers the personal data it possesses to outsourcing service providers, companies packing and delivering the ordered goods for complete fulfilment of the agreement. The goods are packed by [REDACTED], while the delivery is performed by [REDACTED] (agreements enclosed), in accordance with Article 6(1)(b) of GDPR. [...]

The annex contains Agreement No. [REDACTED] on provision of services, which has been concluded between SIA and [REDACTED], and, inter alia, provides that [REDACTED] (performer) in accordance with the Order Form puts the products together and delivers them to final customers using courier services (Sub-Clause 1.3). The Agreement stipulates matters related to confidentiality (Clause 5) and its content corresponds to the agreement concluded between the controller and the processor.

The annex contains Agreement No. [REDACTED] on provision of logistic services, which has been concluded between SIA and [REDACTED], Agreement No. [REDACTED] [REDACTED] on sending and delivery of documents, parcels, packages, which has been concluded between SIA and [REDACTED], Agreement No. [REDACTED] on delivery of correspondence, packages and cargo, which has been concluded between SIA and [REDACTED], Agreement No. [REDACTED] on provision of postal services, which has been concluded between SIA and [REDACTED] parcel delivery Agreement No. [REDACTED], which has been concluded between SIA and [REDACTED]. (DSI 26.06.2019 reg. No.2-4.3/1030-S) (hereinafter—Explanation No.3).

4.9. The Official finds that the Case Files contain the DSI statement of 26.08.2019 with annex No.2-5.1/213. It follows from the information included in the statement and the annex that DSI officials visually inspected the website [REDACTED] and this website contained information about [REDACTED] and an electronic order window for persons from Latvia. Persons should specify their name and phone number when submitting an order. Clicking on the Privacy Policy window at the bottom of the website, information on protection of personal data is available. This information is identical to the one indicated in the Complaint, namely, the one posted on [REDACTED]. When clicking on the Report window at the bottom of the website, it has been stated that the website contains a communication tool, where a text message can be left (for example, feedback can be provided or a question can be asked indicating the person's name and/or surname, phone number and e-mail. The reference to [REDACTED] appears at the bottom of the website. (hereinafter—Statement No.4)

4.10. The Official finds that the Case Files contain an administrative infringement protocol No.FF000113 composed by the Official on 11.09.2019 (hereinafter—the Protocol),

which states that “*SIA in its business—retail sale via mail order or via Internet by processing personal data of customers—natural persons (data subjects)³ (collection, recording, storage, consulting, use, transfer, erasure)⁴ contrary to provisions of Articles 5(1)(1), 5(2) and 12(1) of the General Data Protection Regulation, has not provided the information provided in Article 13 of the Regulation to data subjects, namely, has not ensured observation of the transparency and accountability principle in the processing of personal data of natural persons (customers).*” The administrative infringement in the Protocol is qualified based on Article 83(5)(a) and (b) of the GDPR—for infringement of the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9 of the GDPR and the rights of the data subject pursuant to Articles 12 to 22 of the GDPR (Section 204.⁷(1) of the LAPC—Illegal Operations with a Natural Person’s Data and Section 204.⁸ of the LAPC—Failure to Provide Information to a Data Subject).

After the Protocol preparation, [REDACTED], representative of SIA (hereinafter—the Representative), repeated the already submitted explanations No.1-3 of SIA and testified to the questions asked by the Official that the nature of the infringement was clear to her, that she recognised the infringement and regretted the committed infringement. In addition, the Representative testified that on 06.09.2019 SIA stopped serving customers—natural persons. At the same time, the Representative asked DSI to use the smallest amount of fine, when applying the fine. (DSI 11.09.2019 reg. under No.2-2.3/12) (hereinafter—Explanation No.4).

4.11. The Official finds that the Case Files contain reply letter of SIA of 07.10.2019 to the DSI’s request on the data processing performed by SIA, where SIA explained that “[..] SIA does not own the website [REDACTED], SIA is not a cooperation partner of the legal person [...] [REDACTED]. SIA always provides advertising agencies with advertising samples for preparation of advertisements in accordance with the personal data protection principles of SIA. Sample: [REDACTED].”

SIA explained that “[..] all answers to requests made by the DSI were prepared for SIA by the Auditing Company, about which SIA informed the DSI. Having investigated the situation independently, SIA came to the conclusion that the evidence regarding the fact that the website [REDACTED] specified by DSI has been created in the interests of SIA.” In its reply letter SIA urged DSI to provide SIA with clarifying information or supporting documents that [REDACTED] has been prepared in the interests of SIA.

SIA explained that, “[..] taking into account that the website does not belong to SIA and was not created at the instruction of SIA, trading to customers was not performed through this website. [REDACTED] was not traded through this website. SIA does not receive personal data of natural persons. Contact information of natural persons comes from the call centre, contacts are sent from the call centre in accordance with the goods to be ordered. SIA fulfils orders and sends goods to the specified addresses. Personal data of customers, received through mediation of the cooperation partner, were used only and solely for the purposes of performing the liabilities under the concluded agreement and delivering orders to the customer. [...] Taking into account the amount of information provided by the DSI to SIA, SIA draws the attention of DSI that for the purposes of observing the GDPR, SIA was having an audit, which would allow to comply with all GDPR requirements. Currently, SIA ensures protection of personal data to the extent

³ ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1) of the Regulation);

⁴ ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (Article 4(2) of the Regulation);

provided for by the basis for collection, storage and transfer of personal data—Agreements with cooperation partners and personal data protection policy. SIA needs time to conduct the audit. The audit results have not been received yet. We inform that SIA stopped any advertising at the beginning of September due to short-time financial difficulties. Until the audit opinion is received (we assume that it will be received in the nearest time) and in case it reveals any shortcomings, we will not resume its operations until they are completely rectified.” (DSI 09.10.2019 reg. under No.2-4.3/1671-S) (hereinafter—Explanation No.5).

4.12. The Official finds that the Case Files contain the DSI statement of 09.10.2019 with annex No.2-5.1/248. It follows from the information included in the statement and the annex that DSI officials checked websites [REDACTED] and [REDACTED].

Using the *Google* search, the query of [REDACTED] returned several websites with a similar name, incl. [REDACTED]

[REDACTED] and several other.

When trying to enter [REDACTED], it was stated that at the time of visiting access to the website was denied. By randomly entering websites [REDACTED]

[REDACTED] it was stated that they were similar both visually and in terms of use. The information available on the websites provides evidence of distribution of [REDACTED]. The visual examination has revealed that the websites have an identical electronic order window. Persons should specify their name and phone number when submitting an order. The reference to [REDACTED] appears at the bottom of the websites.

When entering [REDACTED] it has been stated that the website contains information about [REDACTED] and has an electronic order window for persons from Latvia. Persons should specify their name and phone number when submitting an order. Clicking on the Privacy Policy window at the bottom of the website, information on protection of personal data is available in English.

Using *whois.domaintools.com* search for hosts of domains [REDACTED] and [REDACTED], it has been stated that when entering the domain [REDACTED] in the search, the search selects domain [REDACTED]⁵, which was registered on [REDACTED] from a server with an IP address [REDACTED], location [REDACTED], while, when entering domain [REDACTED] in the search, the search selects domain [REDACTED]⁶, which was registered on [REDACTED] from a server with an IP address [REDACTED], location [REDACTED]. (hereinafter referred to as Statement No.5)

5. Regulatory enactment providing for responsibility for the administrative infringement: Article 83(5)(a) and (b) of the GDPR provides that infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: “a” the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9 of the GDPR and the rights of the data subject pursuant to Articles 12 to 22 of the GDPR (Section 204.⁷(1) and Section 204.⁸ of the LAPC).

5.1. In accordance with Section 272 of the LAPC in examining an administrative violation case, shall ascertain, whether the administrative violation has been committed, whether the relevant person is guilty of committing it, whether this person may be subject to administrative liability, whether material losses have been caused, as well as shall ascertain other circumstances which are of importance in deciding the case correctly.

⁵ [http://whois.domaintools.com/\[REDACTED\]](http://whois.domaintools.com/[REDACTED])

⁶ [http://whois.domaintools.com/\[REDACTED\]](http://whois.domaintools.com/[REDACTED])

Therefore, in order to state whether SIA has committed any administrative infringements under Articles 83(5)(a) and (b) of the GDPR (Section 204.⁷(1) and Section 204.⁸ of the LAPC), it is necessary to state that SIA processed personal data without observing provisions of Articles 5, 6, 7, 9 and 12–22 of the GDPR.

5.2. Pursuant to Article 1(1) of the GDPR the purpose of the GDPR is to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Pursuant to Article 2(1) of the GDPR, the GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. The processing of personal data by automated means includes data processing information systems, where persons can be selected based on specific identifiers. A personal data filing system means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Pursuant to Article 4(1) of the GDPR ‘personal data’ means any information relating to an identified or identifiable natural person ('data subject'), while Article 4(2) of the GDPR provides that ‘processing of personal data’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Thus, person’s name, surname, phone number, e-mail and residence or declared address and other information identifying the specific person is considered personal data, while collection, storage, use and transfer of these personal data shall mean processing of personal data within the meaning of Article 4(2) of the GDPR.

Pursuant to Section 4(7) of the GDPR the controller, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data is responsible for compliance of the processing of personal data. In this particular case, SIA is the controller.

Pursuant to Article 6(1) of the GDPR processing shall be lawful only if and to the extent that at least one of the bases referred to in Article 6(1) applies. The GDPR defines six general legal bases: consent, performance of a contract, legal obligation, public interests, protection of vital interests and pursuing of legitimate interests. In addition to the provision of a legal basis, Article 5 of the GDPR should be observed when processing personal data, pursuant to which to protection interests of the person (data subject), the controller shall ensure fair and lawful processing of personal data, as well as processing of personal data only in accordance with the intended purpose and in the necessary scope.

Moreover, observing the accountability principle defined in Article 5(2) of the GDPR, it is the controller who is responsible for the process of processing of such personal data, which can prove that the processing of personal data complies with the requirements of the data protection regulation.

Recital 39 of the GDPR explains that “*Any processing of personal data should be lawful and fair. It 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. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of*

personal data concerning them which are being 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. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."

Furthermore, recital 58 of the GDPR explains that "*the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising.*" Also the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data⁷. In the transparency guidelines in accordance with clear implementation of the transparency principle under the GDPR.

The transparency principle also includes the right of the data subject to be informed and Article 12 of the GDPR provides that the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 [...] in a concise, transparent, intelligible and easily accessible form, using clear and plain language, which means that the controller shall be liable to provide the data subject with the possibility to supervise the processing of data.

Article 12(1) of the GDPR respectively provides that transparent information is information, which is concise, transparent, intelligible. The guidelines provide that the "*Easy availability*" element means that the data subject should not be forced to search for information; they should see immediately, where and how they can access this information, for example, by providing it to them directly, providing a link to it, clearly indicating it as an answer to a question in a natural language, for example, a notice on data protection of several levels, in section "Frequently asked questions", which provide that one of the most effective techniques of the implementation of the transparency principle (which provides the data subject with information on the processing of their data) is publishing on the website of the institution.

Therefore, processing of personal data is recognised to be legal, only if one of the bases and principles specified in these articles exist.

In addition, the Official finds that the controller should also ensure the fulfilment of the requirements of the GDPR, including observation of the rights of the data subject defined in Chapter III of the GDPR.

Recital 63 of the GDPR explains that '*A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. [...] Every data subject should therefore have the right to know and obtain communication in*

⁷ Created based on Article 29 of 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.

particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.'

Articles 13–15 of the GDPR list the rights of the data subject, namely, the data subject shall be entitled to receive the information defined in these articles relating to the processing of the personal data of the data subject. For example, Article 13 of the GDPR defines the right to receive information the controller should provide, if the personal data are obtained from the data subject (for example, to learn the purpose and the legal basis (indicating specific clause of Article 6(1) of the GDPR) of processing of the personal data, or for how long and where the data are stored, whether they are transferred to third parties, etc.), while Article 14 of the GDPR provides, which information the controller should provide to the data subject, if personal data were not obtained from the data subject.

Article 24 of the GDPR defines liability of the controller. In accordance with Article 24(1) of the GDPR, taking into account the nature, scope, context and purposes of data processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Therefore, the controller (the Company) should take relevant technical and organisational measures to protect personal data and prevent their potential illegal processing.

Therefore, in each particular case the controller should evaluate the need for, the legal basis, the purpose of processing of the personal data, types and scopes of the personal data being processed, the potential number of persons, whose personal data are planned to be processes, as well as technical and organisational measures, which secure processing of the personal data, etc.

5.3. The official, based on the conditions of Agreement No. [REDACTED] appended to Explanation No.3, concludes that personal data (name, phone No.) are obtained using advertising and information modules, which is static (with a static image) or animated, graphic information block and/or information block containing text of any form and layout, and has been placed on the website, the selection of which is in competence of SIA, and after ordering [REDACTED], in accordance with provisions of Agreement No. [REDACTED] and Agreement No. [REDACTED], additional data (for example, ordering customer's surname, address, e-mail) are obtained by phone.

At the same time, the Official, based on the information provided in Explanation No.2 and conditions of Agreement No. [REDACTED] and Agreement No. [REDACTED]

[REDACTED] provided in Explanation No.3 and annex thereto, concludes that the controller of the above-mentioned processing of personal data is SIA, because, when selling goods, the operator should use proper conversation scenarios issued by SIA (each conversation scenario is considered an annex and an integral part of the two above-mentioned agreements) and information, which is received by the operator as part of provision of services, is considered confidential and property of SIA, as well as the content of the agreements concluded by SIA corresponds to the agreement concluded between the controller and the processor (includes individual elements defined in Article 28(3) of the GDPR).

This certifies that [REDACTED], the product produced at the commission of SIA, which is sold by SIA, can be ordered at any website selected by SIA, where the advertising and information module created by the cooperation partner will be placed at the instruction of SIA.

Taking into account the aforementioned, the Official concludes that in a situation, when [REDACTED] can be ordered on the websites specified the information in Statement No.2, No.3, No.4 and No.5 providing a reference to [REDACTED] [REDACTED] using an identical advertising and information module, moreover, one of the websites ([REDACTED], created on [REDACTED]) has a Privacy Policy of SIA, which does not meet the requirements of the GDPR, which is confirmed by annex to Statement No.5, and the

controller for the processing of personal data is SIA. It is essential that the websites specified in the Complaint, Statement No.2, No.3 and No.4 have an identical Privacy Policy, where no information about the controller is provided and which does not meet the requirements of the GDPR, as well as the fact that the Invoice appended to the Complaint about [REDACTED] ordered on [REDACTED] specified in the Complaint states the address of SIA. It should be taken into account that as specified by SIA in Explanation No.2, the website [REDACTED], which provides a reference to [REDACTED], is an advertising web page about the product of SIA developed on the instruction of SIA based on a contract.

Visual similarities and usage similarities of [REDACTED] and [REDACTED] should also be noted, as well as the fact that domains of websites [REDACTED] and [REDACTED] have been registered from one and the same server with IP address [REDACTED], the location of which is [REDACTED] and the fact that [REDACTED] was registered on [REDACTED] (before the Case was started and was liquidated during its investigation), but website [REDACTED] was registered on [REDACTED] (during investigation of the Case) and, when providing Explanations No.3 and 4 unambiguously confirmed that SIA is related to [REDACTED], which confirms that SIA organised retail trade of [REDACTED] through [REDACTED].

Having summarised and evaluated all the aforementioned, the Official has concluded that SIA is a controller for the processing of personal data on: [REDACTED] and [REDACTED] on other websites [...] specified in Statement No.5 and in the annex.

The Official also concludes that the information included in Explanations No.1–3 evidences that SIA, as a controller, before the audit of compliance of the processing of personal data with GDPR did not perform the assessment of the personal data processing with the GDPR, therefore the GDPR requirements were not observed in the processing of personal data, including observations of the transparency and accountability principle was not ensured.

The Official critically evaluates the information provided by SIA in Annex No.5, which, in essence, contains contradictory information in SIA's Explanations No.1–4, including the cooperation agreements concluded by SIA, and with regard to the person providing explanation to the DSI, even provides false information (explanations are provided by the member of the board of SIA), therefore she recognises the arguments provided in Explanation No.5 of SIA as an attempt of SIA to avoid responsibility for the failure to perform duties investigated in the Case. It should also be taken into account that the Invoice appended to the Complaint states the address of SIA, indicating inappropriate name of the undertaking ([REDACTED] rather than SIA). Explanation No.5 does not contain an indication that [REDACTED] does not belong to SIA (was created in the interests of SIA), but indicates to probably missing evidences, which would be confirmed by the fact that access to this internet website was denied during investigation.

In addition, the Official indicates that the fact that [REDACTED] does not belong to SIA (was created in the interests of SIA), is not decisive to state the role of SIA in processing of the data. Namely, in several judgements the European Court of Justice recognised that a natural or legal person who exerts influence over the processing of personal data, for his own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller [within the meaning of Article 2(d) of Directive 95/46]⁸ (judgement, 10 July 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, Paragraph 68). It can be stated from the evidences available in the Case that the *purpose* of SIA were retail sales of [REDACTED] to gain profit, which was performed by determining and using a *tool*—[REDACTED], es.therecardio.com, etc.

⁸ In accordance with Article 94 of the GDPR the Directive 95/46/EC is repealed with effect from 25 May 2018. References to the repealed Directive shall be construed as references to the GDPR.

In light of the foregoing, having checked case files, having evaluated circumstances of the Case and the evidences available in the Case jointly with the arguments provided by SIA, the Official states that SIA performed retail sales of [REDACTED] through websites [REDACTED], [REDACTED] and other [REDACTED] websites, was a controller for the processing of personal data of customers—natural persons (data subjects) (collection, recording, storage, consulting, use, transfer, erasure), without observing provisions of Article 5(1)(a), 2 and 12(1) of the GDPR, namely, has not provided the data subject with information provided in Article 13 of the GDPR thus not ensuring observation of the transparency and accountability principle in the processing of personal data of natural persons (customers).

In light of the foregoing, the Official finds that SIA has committed administrative infringements, which are subject to responsibility under Article 83(5)(a) and (b) of the GDPR (Section 204.⁷ and Section 204.⁸ of the LAPC).

5.4. The Official finds that the guilt of SIA in commitment of the administrative infringements under Articles 83(5)(a) and (b) of the GDPR (Section 204.⁷(1) and Section 204.⁸ of the LAPC) is proved by: 1. Complaint by [REDACTED]; 2. Explanations No.1–5 of SIA, 3. Protocol, 4. DSI Statements No.1–5.

6. Decision of the institution (official), which examined the administrative infringement case:

6.1. In accordance with Article 83(2) of the GDPR, when deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; b) the intentional or negligent character of the infringement; c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; e) any relevant previous infringements by the controller or processor; f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; g) the categories of personal data affected by the infringement; h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

Recital 148 of the preamble to the GDPR explains that '*in order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation. In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Due regard should however be given to the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor. The imposition of penalties including administrative fines should be subject to appropriate procedural safeguards in accordance with the general principles of Union law and the Charter, including effective judicial protection and due process.*'

Pursuant to Section 22 of the LAPC, administrative sanction is the means of liability and shall be applied in order to educate a person, who has committed an administrative violation, in the spirit of law abiding and respecting provisions of social life, as well as in order to prevent the violator of the rights, as well as other persons, from committing new violations.

Pursuant to Section 32 of the LAPC, in imposing a sanction the nature of the committed violation, the personality of a violator, the degree of his or her culpability, the liability mitigating and aggravating circumstances shall be taken into account.

Pursuant to Section 35 of the LAPC, if one person has committed two or more administrative violations, an administrative sanction shall be imposed for each violation separately. If a person has committed administrative violations, which have been determined simultaneously, and they are examined by one and the same institution (official), administrative sanction shall be imposed within the framework of that sanction which is provided for the more serious violation. In such a case a basic sanction may be supplemented by any of the additional sanctions, which are provided for in the Sections, which determine liability for any of the violations committed.

6.2. When determining the sanction, the Official takes into account the following aspects of the infringement: 1) the nature, gravity and duration—in this particular case, SIA, by performing retail sales of [REDACTED] through several websites, processed personal data of customers—natural persons (data subjects)—collection, recording, storage, consulting, use, transfer, erasure) without observing provisions of Article 5(1)(a), 2 and 12(1) of the GDPR, namely, has not provided the data subject with information provided in Article 13 of the GDPR, thereby not ensuring observation of the transparency and accountability principle in the processing of personal data of natural persons (customers) at least since 10.07.2018 (the date, when the purchase of [REDACTED] by [REDACTED] was registered) and until 06.09.2019 (the date, when according to the information provided by the representative of SIA in Explanation No.4 SIA stopped serving customers—natural persons); 2) the intentional or negligent character of the infringement—in this particular case the processing of the personal data by SIA without providing data subjects with the information defined in the GDPR, shall be considered intentional; 3) the number of data subjects affected—in the Case the Official has not managed to learn the specific number of the data subjects affected. In this particular case, the Official, taking into account that [REDACTED] was distributed through several websites, incl. [REDACTED]

[REDACTED] and other [REDACTED] websites that are oriented to consumers—natural persons in several European Union Member States, and in accordance with the available information SIA has been registered since 26.05.2015 and financial indicators for the last submitted year 2017 show the turnover of SIA in the amount of EUR 12,470,064.00, the Official has come to the conclusion that the number of affected data subjects was considerable. 3) Previous infringements by the controller—in this particular case, SIA was not previously administratively punished for committing the infringement examined in this decision; 5) The degree of cooperation of the company with the supervisory authority—at first, SIA cooperated with the institution, but in Explanations No.5 provided information contradictory to that provided in SIA's Explanations No.1–4 and has not provided the supervisory authority with information, since when (specifying the exact date) SIA has been selling [REDACTED] to customers—natural persons using the website [REDACTED] customers—natural persons, of which countries (specifying each) were sold [REDACTED] by SIA and specify the exact number of customers—natural persons, who ordered [REDACTED] from SIA and whom SIA has sold and delivered since SIA has started to distribute [REDACTED], using [REDACTED] 7) the manner in which the infringement became known to DSI—complaint of a data subject transferred to DSI by other supervisory authority; 8) any other aggravating or mitigating factor applicable to the circumstances of the case—the Official finds that financial benefits have been gained from the infringement indirectly.

Taking into account the aforementioned and the purpose of the administrative sanction, the Official concludes that the fine provided for within the scope of the sanction for infringement under Article 83(5)(1) of the GDPR (Section 204.⁷(1) of the LAPC) and Article 83(5)(b) of the GDPR (Section (204.⁸) amounting to 1% of the net turnover of 2017 (EUR 12,470,064) at the end of the period (last available data) should be imposed on SIA.

In light of the foregoing, based on Article 83(2) of the GDPR, Sections 236.¹⁰, 275(1)(1), 276(1) and (2), 279(1), 281 of the LAPC, the Official

decides:

1. To impose on Limited Liability Company [REDACTED], registration number [REDACTED], an administrative fine of EUR 124,700.64 (*one hundred and twenty-four thousand seven hundred euro 64 cents*) for the committed infringement, which is subject to responsibility under Article 83(5)(a) of the GDPR (Section 204.⁷(1) of the LAPC).

2. To impose on Limited Liability Company [REDACTED], registration number [REDACTED], an administrative fine of EUR 124,700.64 (*one hundred and twenty-four thousand seven hundred euro 64 cents*) for the committed infringement, which is subject to responsibility under Article 83(5)(b) of the GDPR (Section 204.⁸ of the LAPC).

3. Based on Article 35(2) of the Latvian Administrative Procedure Code, to impose on Limited Liability Company [REDACTED], registration number [REDACTED], the final fine of EUR 150,000 (*one hundred and fifty thousand euro and 00 cents*).

The decision can be appealed by submitting a complaint to the DSI director at Blauma iela 11/13-15, Riga, LV-1011, within 10 (ten) working days of the day of notification of (receiving) the decision.

The fine can be paid in any bank institution. Details for payment of the fine:

Beneficiary: State Treasury

Registration No.: 90000050138

Account No.: LV69TREL1060191019200

Beneficiary's BIC code: TRELLV22

Notes: Specify the date and number of this decision.

8. Signature

Data State Inspectorate
Personal Data Processing
Supervision Department Head
[REDACTED]

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

Background information

Date of final decision: 8 November 2019

LSA: LV

CSAs: All SAs

Legal Reference: Transparency (Article 12), Information (Articles 13 and 14)

Decision: Infringement of the GDPR, Fine

Key words: Transparency, Information, E-commerce, Identity of the controller

Summary of the Decision

Origin of the case

The complainant alleged that he did not receive information on the identity of the controller before submitting his order on the online retail platform. Moreover, the complainant contended that the privacy policy available on the website was not in conformity with the GDPR.

Findings

During its investigation, the LSA found that the controller was a Latvian company performing retail sales through several websites, including the one used by the complainant to order his goods.

After establishing the identity of the controller, the LSA found that the privacy policy on the website did not provide information on the identity of the controller, the legal basis of the data processing, its purposes and the way data subjects' consent is collected.

Decision

The LSA found that the controller did not comply with his obligations under the GDPR and imposed a fine of 150,000 euros.

Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

Reference is made to the complaint (registered internally with file number CDP/IMI/LSA/2/2019) received from the Spanish Data Protection Agency (Agencia Española de Protección de Datos or AEPD) concerning [REDACTED] the “complainant”), who is alleging tha

[REDACTED] (“the bank” or “the controller”) breached her data protection rights, as enshrined under the General Data Protection Regulation – Regulation (EU) 2016/679 (“GDPR” or the “Regulation”). The complainant contended that she has been receiving several unsolicited calls to the fixed line number [REDACTED] corresponding to her place of residence even after having submitted a right of erasure request and such erasure confirmation was made by the controller. It has to be noted that the owner of the concerned phone number is [REDACTED] ather of the complainant and that the erasure request was therefore submitted by [REDACTED]

INVESTIGATION

As part of the investigation process, through emails dated 17th January 2019 and 17 May 2019 respectively, the Commissioner requested the controller to put forward its submissions on the allegation raised by the complainant. Submissions were received on the 25th January 2019 and on the 24th of May 2019, and included the following principal arguments:

- a. on 7th August 2018 the bank approved a 30 days loan to a client, namely [REDACTED] [REDACTED] the “client” or “the borrower”);
- b. when submitting the online loan application, the client provided the bank with two phone numbers one of which being [REDACTED]

- c. on 6th September 2018, the day the loan was due for payment, the bank was informed by the client that she would have been able to pay the loan only on the 1st of October 2018;
- d. starting from the 13th of September the bank tried to contact the client on the number mentioned above without knowing that the number corresponds to the complainant's residence and not to its client. During these calls the complainant explained to the data controller that she was not the person they were looking for and that she didn't know the bank's client [REDACTED]
[REDACTED] was invited to submit, by using a form available on the controller's website, a right of erasure request. It has to be noted that while the complainant is the user of the phone number concerned, the phone number owner is [REDACTED]. On the 23rd of October 2018 the bank received the erasure request from [REDACTED] and on the 2nd of November an email confirming the phone number erasure from the data controller's database was received by [REDACTED]
- e. the controller has only one database where phone numbers, belonging to bank's clients, are recorded in the corresponding client's records. Once [REDACTED] residence phone number was erased from the bank's records, the phone number would no longer appear in the bank's database. It resulted that the controller erased the phone number from its database immediately after the data subject's erasure request on 23rd October 2018, and it follows that the bank's personnel was not in any way able to make use of the phone number after this date;
- f. from the controller's call logs it transpires that the last call to the complainant's residence phone number was made on 25th October 2018 at 15.22 while from the complaint's report it appears that further unsolicited phone calls were still received between the 2nd of November and the 9th November 2018 (date when the complaint was filed with the AEPD);
- g. from the complainant's report it also transpires that, during one of these phone calls, the complainant was erroneously informed that she was still receiving unsolicited calls as the concerned phone number, while it was erased from one database on the 23rd of October 2018, was still recorded in another data controller's database. The complainant was thus invited to submit a second erasure request to delete the number also from this database;
- h. the complainant sent a second erasure request on the 5th November 2018. The answer to this request, that was sent by email on the 6th of November, was meant just to reconfirm the erasure made on the 23rd of October. However, the content was written in such a way that led the

complainant to assume that this was a new erasure confirmation relating to the data recorded in the other data controller's database. This assumption was not correct as the bank has only one database (please refer to paragraph "e");

- i. this Office eventually instructed the data controller to send a further erasure confirmation to the complainant. This third erasure confirmation was sent to [REDACTED] on the 11th of February 2019 and a copy was also received by this Office on the same day;
- j. taking into consideration that the complainant's residence phone number was fraudulently provided to the bank by its client, the bank cannot exclude the possibility that the complainant's residence's phone number was provided by the same client, also to other entities/lenders and that these entities/lenders may make use of it after the 25th October 2018.

DECISION

On the basis of the foregoing the Commissioner is hereby instructing the data controller to implement the appropriate technical and organizational measures to make sure that personal data are accurate and, where necessary, kept up to date and that every reasonable step is taken to ensure that personal data that are inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay.



Information and Data Protection Commissioner

Today, the *17th* day of June, 2019

Summary Final Decision Art 60

Complaint

Compliance Order to Controller

Background information

Date of final decision:	7 June 2019
LSA:	MT
CSAs:	ES
Legal Reference:	Right to erasure (Article 17)
Decision:	Compliance order to controller
Key words:	Right to erasure, Data subject rights, Accuracy

Summary of the Decision

Origin of the case

A Spanish data subject filed a complaint with the Spanish SA as she was receiving unsolicited phone calls even after having filed an erasure request and such erasure had been confirmed by the data controller.

Findings

The complainant's phone number was fraudulently provided to the controller by one of its clients. Since the controller was not aware of this, it tried to contact the client on such phone number. The complainant filed a right of erasure request. During a phone call, the controller erroneously informed the complainant of the need to submit a second erasure request to delete the number from another database held by the controller, whereas only one database existed. From the call logs provided by the controller it transpires that the complainant phone number was erased from the controller's database immediately after the first erasure request. All the erasure requests from the complainant were followed by erasure confirmations sent by the controller. The controller couldn't exclude the possibility that the complainant's residence's phone number was fraudulently provided by the same client, also to other entities/lenders and that these entities/lenders may make use of it.

Decision

The LSA instructed the data controller to implement the appropriate technical and organisational measures to make sure that personal data are accurate and, where necessary, kept up to date, and

that every reasonable step is taken to ensure that personal data that are inaccurate, having regards to the purposes for which they are processed, are erased or rectified without delay.

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision: 4 March 2019

LSA: MT

CSAs: IE

Legal Reference: Right to erasure (Article 17)

Decision: No violation

Key words: Right to erasure, right of access request, exercise of the rights of the data subjects

Summary of the Decision

Origin of the case

The complainant made a right to access/erasure request to the controller. The controller requested the complainant to confirm her identity but she failed to do so.

The controller has erased the complainant's personal data accordingly to its privacy policy and taking into consideration a still existing "Compromise Agreement" between the controller and the complainant. Concerning the right of access request, the only reason why the information was not provided revolves around the complainant's failure to verify her identity with the controller. The complainant then contended that the controller did not accede to the right of access request.

Findings

The LSA assessed that the controller satisfied the complainant's right of erasure request to the extent permissible by the applicable laws, including but not limited to, employment legislation.

The LSA found that the controller took all the necessary steps to handle the complainant's right of access. The only reason why the information was not provided, was due to the complainant's failure to verify her identity with the controller (the email she was using was not known to the controller).

Decision

The LSA decided that the controller did not infringe the provisions of the GDPR, and consequently dismissed the compliant.

[REDACTED]

[REDACTED]

Vs

[REDACTED]

COMPLAINT

Reference is made to the complaint (registered internally with file number CDP/IMI/LSA/6/2019) received from the Spanish Data Protection Agency (Agencia Española de Protección de Datos or AEPD) concerning [REDACTED] (“the complainant”) who is alleging that [REDACTED] [REDACTED] (“the controller“ or [REDACTED] breached her data protection rights, as enshrined under the General Data Protection Regulation – Regulation (EU) 2016/679 (“GDPR“ or the “Regulation”). The complainant contended that her personal data were inserted in [REDACTED] without providing her, at the time the data were obtained, the required information in terms of Article 13 of the GDPR.

INVESTIGATION

From the investigation carried out by this Office and from the controller’s submissions, it transpires that the controller took all the reasonable steps to provide the complainant with the required information in terms of Article 13 of the GDPR.

In the general Terms and Conditions of the contract between the [REDACTED] and the complainant, which were accepted by the complainant [REDACTED], clause 11(ii) states (the translation from Spanish to English has been provided by the data controller, and is being reproduced *verbatim*): “*The client is informed and agrees to be required to pay in writing through SMS, email and / or postal mail to the address and phone number provided by him to [REDACTED] or, if he has changed them, to the new address and / or telephone number communicated to [REDACTED]. Said requirement shall be prior to the inclusion in the files [REDACTED] in accordance with RD 1720/2007, of December 21*

by which the Regulation of development of the Organic Law 15/1999 of December 13 on protection of personal data is approved, the Maltese Law on data protection and the European Directive 95/46/EC, of the Parliament and the Council of Europe, of 24 October and other applicable regulations.

To this end, taking into account the nature of distance contracting to which the parties agree and to the uses of this type of contract, the client acknowledges that [REDACTED] by using distance techniques means that [REDACTED] can get in touch with him for any matter (including [REDACTED] [REDACTED]), arising from the contractual relationship that binds them through any of these channels, especially SMS and electronic mail, expressly stating that the data that client enters in the [REDACTED] application are valid and are operational, especially email.

Once the period established in the previous made [REDACTED] has expired, the client is informed and agrees that, in case of continuing with the [REDACTED]

[REDACTED] client's data may be included in the [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

In addition:

- [REDACTED] was sent by post to the complainant's address by the controller. In the letter the complainant was given ten (10) more days to proceed with the [REDACTED] failing which, she was also informed that her personal data would be included in [REDACTED]
[REDACTED];
- warning emails and SMSs informing the complainant that [REDACTED] would lead to the inclusion of her personal details [REDACTED] were sent respectively on 11.01.2018 and 10.02.2018 (for emails), and on 17.12.2017 and 29.12.2017 (in case of SMSs).

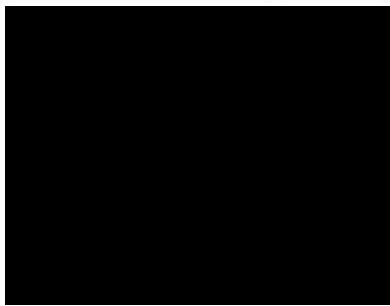
Moreover in the "Terms and Conditions" available on the data controller's website, at paragraph 26.11.4, the following information can be found: "*Without prejudice to the generality of the above clauses, you acknowledge that the [REDACTED] shall transfer information regarding your [REDACTED] (including your Personal Data) to third-entities which process information on [REDACTED] of persons, and also that the [REDACTED] shall place information regarding your [REDACTED] (including your Personal Data) on the [REDACTED]*

[REDACTED] You also acknowledge that the [REDACTED] shall transfer information

regarding your [REDACTED] (including your Personal Data) to third entities for the purpose of [REDACTED].

DECISION

On the basis of the foregoing the Commissioner considers that the complainant was adequately informed pursuant to Article 13 of the GDPR and thus considers the case as closed.



Saviour Cachia
Information and Data Protection Commissioner

Today, the 5th day of August 2019

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	5 August 2019
LSA:	MT
CSAs:	DK, ES, FI, FR, LV, NO, SE
Legal Reference:	Information to be provided where personal data are collected from the data subject (Article 13 GDPR)
Decision:	No violation
Key words:	Right to information, prior information, rights of data subjects

Summary of the Decision

Origin of the case

The complainant contended that her personal data were inserted in the insolvency register of a third party without having been provided the required information, in accordance with Article 13 GDPR, at the time her data were obtained.

Findings

The LSA found that all relevant information was provided to the complainant through the general Terms and Conditions of the loan contract, which she accepted before the loan was granted to her. Additionally, the information that her personal data would be inserted in the insolvency register was communicated to her through a ‘requirement of payment’ letter and warning emails and SMS texts. The same information is also available on the controller’s website.

Decision

The LSA found that the complainant was adequately informed pursuant to Article 13 GDPR.

Information and Data Protection Commissioner

[REDACTED]
Vs
[REDACTED]

COMPLAINT

Reference is made to the complaint (registered internally with file number CDP/IMI/LSA/17/2019) received from the Polish Office for Personal Data Protection concerning [REDACTED] ("the complainant") who is alleging that [REDACTED] ("the controller" or "[REDACTED]") breached her data protection rights, as enshrined under the General Data Protection Regulation¹ ("GDPR" or the "Regulation"). The complainant contended that the controller did not comply with her right of access request in terms of Article 15 of the GDPR within the established thirty (30) days' time frame. From the information provided by the complainant, it transpires that she filed her right of access request on the 3rd of October 2018 and on the 5th February 2019, the date when she filed the complaint with the Polish DPA, the controller did not yet provide her with a reply.

INVESTIGATION

As part of the investigation process, on the 26th of July 2019, through an email, the Commissioner requested the controller to put forward their submissions on the allegation raised by the complainant. The submissions, that were received through an email on the 9th of August 2019, contained a letter that supposedly was sent to the complainant on the 4th of October 2018, the day after the complainant's request was received by [REDACTED], together with the file containing the copy of her data. As this letter was in the Polish language, the Commissioner kindly requested the controller to provide an English translation.

On the 12th of August 2019, the Commissioner was informed, through an email, that while working on the English translation, [REDACTED] realised that neither the letter nor the file containing the personal data was ever sent to the complainant, due to (verbatim) "*a wrong use of the security classification settings by the [REDACTED]'s employee with access to the mailbox ([REDACTED]) used to correspond with the said customer [the complainant]*". The security classification was set to be

¹ Regulation (EU) 2016/679 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)

“Internal only”. This setting does not allow communications to be sent outside the organization’s network domain.

Following an internal investigation on this matter, the controller found out that (verbatim) “*after internal organizational changes the person in charge of this particular customer request left the company without concluding the case and ensuring that a reply was properly sent to the customer. For this reason, the file containing the list of personal data processed by [REDACTED] has not reach the customer, together with the usual letter sent to customer’s following a Data Subject Access Request*”. The same day the error on the email setting was discovered, meaning on the 12th August 2019, in order to immediately address the incident, [REDACTED] sent the complainant another email apologising for the late reply, attaching a letter giving details about the processing of personal data, together with the requested information in the form of a PDF file.

On the 13th of August, the Commissioner requested a copy of the above-mentioned email and attached PDF file, as evidence that action has been taken in that regard. The copy was eventually received on the 14th August 2019.

The controller was further requested, through an email dated 19th August 2019, to put forward further submissions on the organizational and security measures implemented following this incident, to prevent such a similar incident from occurring again. From this submission, received on the 23rd August 2019, it transpires that now [REDACTED] has extended its backup continuity procedure to ensure that customers’ requests to exercise their rights under the GDPR are addressed promptly, (verbatim) “*The procedure is designed to ensure an adequate follow-up and mirroring of the tasks within the Customer Service Unit. All the customer requests are now followed-up by two persons, one been the main contact (principal) and a second person following the correspondence as a back-up, with the capability to intervene when the principal is not capable of doing so. The principal is a senior Customer Service Agent while the “back-up” is either a Senior Team Member or a senior customer service officer having experience and knowledge on the various internal procedures regarding the types of requests received at by the Customer Services team. In case the first contact is away, sick or unavailable, the back-up is able to take over the tasks if these are not finalized or achieved, thereby closing of the customer requests without impacting the customer negatively. Controls and checks have been integrated within the process in order to avoid such an incident from occurring again in the future*

DECISION

On the basis of the foregoing the Commissioner considers that [REDACTED] did not have adequate procedures in place to deal with subject access requests, resulting with the complainant actually deprived of her right to access her data within the timeframe stipulated within the Regulation. Consequently, **the data controller is found to be in violation of Article 15 of the GDPR.**

After having taken into consideration:

- the controller's degree of cooperation with this Office;
- that the controller took immediate action to comply with the complainant's request as soon as the error in the security settings of the mail box used to communicate with the complainant was discovered;
- that the controller has now in place a better procedure introducing measures to improve the process to deal with the customers' requests to exercise their rights under the GDPR and to keep within the legal timeframes;

and also giving due regard to the circumstances contemplated under Article 83.2 of the GDPR and taking into account Article 83.1, [REDACTED] is hereby being served with an administrative fine of eight thousand euros (€ 8,000).

The administrative fine shall be paid to the Commissioner within twenty-five (25) days from receipt of this decision.

In addition, [REDACTED] is hereby being instructed to implement the appropriate technical measures to further enhance the measures already in place.

A copy of this decision is also being sent to the Polish Office for Personal Data Protection.



Saviour Cachia
Information and Data Protection Commissioner

Today, the 28th day of October, 2019

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

Background information

Date of final decision: 28 October 2019

LSA: MT

CSAs: PL

Legal Reference: Right of access (Article 15)

Decision: Infringement of Article 15 GDPR

Key words: Right of access, Data subjects' rights, Data subject access request, Bank, Technical and organisational measures

Summary of the Decision

Origin of the case

The complainant filed a complaint with the CSA contending that the controller did not comply with her access request within the established 30 days' period.

Findings

The LSA found that a letter and a file containing the copy of the complainant's data were supposed to be sent to her on the day following the request. However, the email was erroneously categorised as "internal only", which resulted in a failure to send such letter and file to the complainant. Furthermore, the employee with access to the relevant mailbox left the company without ensuring that the complainant received a reply. Following the LSA's investigation and the discovery of the mistake, the controller provided the complainant with a letter giving details about the processing of her data and the file containing the requested information.

Furthermore, the LSA requested the controller to submit details on the organizational and security measures implemented to avoid similar incidents in the future. To ensure an adequate follow-up of the access requests, the controller improved its back-up continuity procedure under which the back-up person would intervene if the main contact was not capable of complying with the client's request.

Decision

The LSA found that the controller infringed Article 15 GDPR by not having adequate procedures in place to deal with subject access request, thus depriving the complainant of the right to access her data within the established timeframe. As a result, and also in light of several mitigating circumstances, the controller received an administrative fine of 8,000 euros. The LSA also instructed the controller to implement the appropriate technical measures to enhance the organizational and security measures already put in place.

[REDACTED]
Vs
[REDACTED]

COMPLAINT

Reference is made to the complaint (registered internally with file number CDP/IMI/LSA/27/2018) received from the Berlin Commissioner for Data Protection and Freedom of Information (the “concerned supervisory authority” or “CSA”) concerning [REDACTED] (“the complainant”) who is alleging that [REDACTED] (“the controller” or “[REDACTED]”) breached his data protection rights, as enshrined under the General Data Protection Regulation¹ (“GDPR” or the “Regulation”). The complainant contended that the controller was still processing his personal data for the purposes of sending him marketing communications despite the fact that he has revoked his consent.

In particular the complainant wanted to have confirmation from the data controller that his first email dated 30th November, 2017, by which he revoked his consent to use both his email addresses and his mobile phone number for the purpose of sending marketing communication, had been received by the controller.

It has to be noted that when the complaint was lodged for the first time with the Office of the Information and Data Protection Commissioner (“IDPC” or “Commissioner”), on the 13th of September 2018, the IDPC requested the controller to confirm that its main establishment was in Malta. Despite the controller’s positive answer, following a preliminary investigation, it transpired that the controller had just an office registered in Malta but it did not have its main establishment within the Maltese territory. The CSA was informed of this outcome of the preliminary investigation.

On the 23rd July 2019 the CSA informed this Office of the change of the data controller’s registered address. From an unannounced IDPC visit to the new data controller’s premises to deliver a request for submission by hand, it transpires that currently the controller has an office and some employees in Malta. However, during this visit it was not possible to establish whether the Malta office is in fact the

¹ Regulation (EU) 2016/679 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)

controller's main establishment as when we asked for the data protection officer, at that time, he/she was not present.

INVESTIGATION

As part of the investigation process, on the 13th of September 2018 the Commissioner requested the controller through an email to confirm that its main establishment was in Malta. Following its positive reply, the Commissioner requested the controller to put forward its submissions on the allegation raised by the complainant, through a registered letter dated 11th October 2018. As the submissions, that were received through email, only contained information that was already known, which was part of the complaint, further submissions were requested on the 25th of March, 2019. In view that no reply was forthcoming, a reminder in the form of registered mail was sent on the 8th April, which according to MaltaPost plc, was not delivered "*due to addressee not available*". Eventually our investigations led to another different e-mail address for the controller, and another e-mail was sent on the 23rd of April. A reply was received through email on the 2nd of May, 2019. Further documentation was requested on the 26th July 2019 to which a reply was received on 1st of August, 2019.

The Commissioner notes that the long time it has taken for the Controller to be contacted and eventually reply to all the requests made by his Office, and the fact that even though the Commissioner had to resort to using registered mail and still no reply was forthcoming, it is being highlighted that the controller's degree of cooperation with this Office is not in line with what is expected under the GDPR.

The submissions included the following principal arguments:

- The controller confirmed that they were not able to find the first email sent by the complainant on the 30th of November 2017 on their server, and therefore cannot confirm whether this email was ever received or otherwise. The controller also stated that there is a possibility that the email, in case it was received, was not dealt with properly and, this might be the reason why it is not stored on its system. In any case the controller did not comply with the complainant's request within the legal time and, as a consequence, the complainant was still receiving marketing communications after the 30th of November, 2017;
- For privacy and security reasons the controller requires registered customers to get in contact by using the email address provided when opening their accounts. The email address used by the complainant when opening his account was [REDACTED]. When sending the email on the 30th of November, the complainant used this email address. It has to be noted that the complainant has other four (4) email addresses namely: j[REDACTED],

[REDACTED] that are not linked to his account

with the controller;

- The controller confirmed that they were able to identify sixteen (16) cases in which marketing communications were sent to the email address [REDACTED] after the 30th of November, 2017. Besides these sixteen cases the controller was not able to find any other marketing communication sent to the complainant, neither before the 30th November, 2017, nor after;
- It has to be noted that the complainant is claiming that the controller has used his personal data (email address and mobile number) to send him marketing communication after the 30th of November, 2017, which amounted to between forty two (42) and forty five (45) instances. The complainant provided this Office with a copy of the marketing email received on June 11th 2018;
- From the submissions dated 2nd May 2019, it transpires that after having re-assessed its communication system the controller was not able to find any marketing communications sent to any of the other email addresses pertaining to the complainant and not associated to his account with the controller, thus the controller is of the opinion that such emails have not been sent;
- Following the receipt of the marketing communications after the 30th of November, 2017, the complainant sent various emails to the controller soliciting to stop sending unsolicited marketing communications. In sending these emails the complainant randomly used all his email addresses mentioned above, and not only the email address he used to open his account. As a consequence, according to the initial controller's submissions, the controller was not able to identify the complainant and thus could not satisfy his requests;
- On the 24th of June, 2018, the complainant sent a further email to the controller requesting once more to stop the processing of his personal data for the purpose of sending marketing communications. Despite the fact that the email was sent using the email address [REDACTED] (and not the email address used by the complainant to open his account), on the 25th of June, 2018 the controller blocked the complainant's account from receiving any marketing communications. After this date no marketing communications have been sent to the complainant by the data controller;
- The controller has revised, redesigned and implemented internal procedures relating to the handling of data subject right requests.

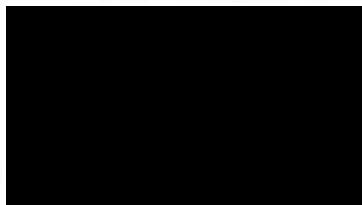
DECISION

On the basis of the foregoing, the Commissioner considers that the data controller did not have adequate procedures in place to deal with the complainant's request to exercise his right to object to processing operations, resulting with the complainant actually being deprived of this right. Furthermore, the Commissioner views that there was lack of co-operation in dealing with this case. Subsequently the controller is found to be in violation of Articles 21 and 31 respectively of the GDPR, and after giving due regards to the circumstances contemplated under Article 83.2 of the GDPR and taking into account Article 83.1, [REDACTED] is hereby being served with an administrative fine of fifteen thousand Euro (€ 15,000).

The Commissioner also considers that the controller's inability to deal with the data subject's complaints, in particular, the lack of procedure to handle the right of erasure request, led to the sending of unsolicited communications to the complainant. The controller is therefore also found to be in breach of regulation 9 of Subsidiary Legislation 586.01 of the Laws of Malta and pursuant to regulation 13 thereof, the data controller is hereby being served with an administrative fine of two thousand Euro (€ 2,000) for this violation.

The administrative fines shall be paid to the Commissioner within twenty-five (25) days from receipt of this decision.

A copy of this decision is also being sent to the Berlin Commissioner for Data Protection and Freedom of Information



Saviour Cacnia

Information and Data Protection Commissioner

Today, the *10th* day of October 2019

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

Background information

Date of final decision:	10 October 2019
LSA:	MT
CSAs:	DE-Berlin, NL, NO, SE
Legal Reference:	Right to object (Article 21), Cooperation with the supervisory authority (Article 31)
Decision:	Infringement of Article 21 and Article 31 GDPR
Key words:	Right to object, Cooperation with the supervisory authority, Exercise of data subjects' rights, Marketing communications

Summary of the Decision

Origin of the case

The complainant lodged a complaint with the CSA alleging that the controller kept sending marketing communications to the complainant even though he had previously objected to the processing of his data for marketing purposes.

Findings

The preliminary investigation by the LSA was aimed at ensuring that the controller's main establishment was in its country.

The controller as internal procedure accepted any requests from data subjects only when the requests were made by using the same email address the users have used to open their account.

Through its investigations, the LSA found out that the controller could not find the first email sent by the complainant to object to the processing of his data for marketing purposes even if this email was sent from the email address used by the user to open his account. The data controller admitted that there was a possibility that the email had not been received or had not been dealt with properly.

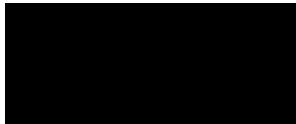
Following the receipt of further unsolicited marketing communications, the complainant objected several more times. These emails were sent from email addresses different from the one used to open his account. Even if the controller was thus not able to comply with the data subject's request as he

could not identify him, the controller decided to block the complainant's account from receiving marketing communications. From the investigation it transpired that the controller did not have any internal procedures for the handling of data subjects' requests.

In addition the controller did not cooperate with the LSA that had to wait months to receive the requested submissions.

Decision

The LSA found that the controller infringed Article 21 by not having adequate procedures put in place to deal with the complainant's request to exercise his right to object. The controller also infringed Article 31 GDPR by not cooperating with the LSA. Consequently, the LSA imposed an administrative fine of 15,000 euros on the controller. A 2,000 euro administrative fine was also imposed on the controller for having breached several provisions of national law relating to unsolicited communications.



Unntatt offentlighet:
Offl §13 jfr Fvl §13 nr 1

Deres referanse

Vår referanse
19/01274-6/AKU

Dato
18.05.2020

A56ID 64543 – Cross-border case - Protector Forsikring ASA – Closure of case.

We refer to your complaint received by the Danish Data Protection Authority (DPA) on February 10th 2019 against Protector Forsikring ASA, about their refusal to provide access to an opinion prepared by the Protector Forsikring Danmark's doctor.

The Danish DPA sent inquiry to Protector Forsikring Danmark in a letter dated 13 March 2019, to establish if this was a cross-border case and which authority should handle the complaint. Protector Forsikring Danmark answered on April 1st 2019 that Protector Forsikring ASA in Norway is data controller in the meaning of the General Data Protection Regulation (GDPR). They confirmed that the head office in Norway makes decisions in relation to the purposes and means of processing personal data in Protector Forsikring Danmark and has the power to have those decisions implemented.

Therefore, the Norwegian Data Protection Authority took over as Lead Authority handling your complaint on April 11th 2019.

We requested information from Protector Forsikring ASA in a letter dated 9 December 2019 and asked among other things why they did not regard the personal data in the doctor's opinion as covered by the right of access in GDPR art. 15 and about their routines for handling of access requests.

Protector Forsikring answered in a letter dated 19 December 2019 that they are of the opinion that you should get access to the personal data you requested and that they will send a copy of the personal data to your attorney on 20 December 2019 at the latest. They also explained their routine of access requests.

In the light of this information we decide to close this case. If you disagree with our decision you have the right to send a complaint to us pursuant to Norwegian Public Administration Act section VI, within three weeks from the day you received this letter.

We apologize for the excessive time it has taken to handle your case.

With kind regards,



Kopi til: Datatilsynet i Danmark, Borgergade 28, 5 sal, 1300 København, DK
PROTECTOR FORSIKRING ASA, Postboks 1351 Vika

Summary Final Decision Art 60

Complaint

No violation

EDPBI:NO:OSS:D:2020:108

Background information

Date of final decision: 18 May 2020

LSA: NO

CSAs: DK, FI, SE

Controller: Protector Forsikring ASA

Legal Reference: Right to rectification (Article 16), Right of access (Article 15)

Decision: No violation

Key words: Access request

Summary of the Decision

Origin of the case

The complainant initiated the complaint against the controller as a result of their refusal to provide access to personal data.

Findings

The LSA requested information from the controller including why they did not regard the personal data in the opinion of the doctor in connection with the complainant's insurance case as covered by the right of access and queried their routine for handling data access requests.

In response, the controller agreed that the complainant should be granted access to their personal data as requested. They further explained their routine for handling access requests.

Decision

The LSA closed the case since the data subject was granted access.

Thank you for your email of 22 January 2018.

Our view

I have considered the information available in relation to this complaint and I am of the view that [REDACTED] has complied with its data protection obligations.

You have explained that following receipt of our email you looked at both customer's – [REDACTED] ("Customer A") and [REDACTED] ("Customer B") – histories in its fraud engine. You provided us with the following information:

1. Both customers logged on from the same device (Device ID [REDACTED]) – Customer A logged onto this device on the 11 July 2018 and the 26 July 2018, Customer B logged onto this device on the 30 July 2018.
2. Both customers have logged on from the same IP address: IP Address [REDACTED] – Customer A logged on from this IP address on the 26 July 2018, Customer B logged on from this IP address on the 30 July 2018.

You have also explained that a user's account on the [REDACTED] website does not store payment card details. Instead, "payment tokens" are stored in a database – a payment token is a unique identifier for a payment card. Your organisation's fraud engine and its payment gateway will each give a payment card a payment token. Payment tokens are not shared with users.

It is my understanding that the fraud engine will give a payment card the same payment token even if that payment card is used by many different accounts or users. The payment gateway will give each individual account a separate token even if several accounts use the same payment card.

If a user transacts on the website, payment tokens are used to make a call to the payment gateway. Of a user's 15 or 16 digit card number (depending on the card type), the only information that is logged in a user's account and that a user would see are the last two digits of their payment card.

We are satisfied with the response you have provided and based on the information we now have available it appears likely that the data subject has used the same device as a third party.

We will now close this case with no further action. Thank you for your cooperation whilst we dealt with the matter.

Yours sincerely

[REDACTED]
Lead Case officer
Information Commissioner's Office
[REDACTED]

ICO Statement

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	22 June 2019
LSA:	UK
CSAs:	IE
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No violation
Key words:	Data Breach

Summary of the Decision

Origin of the case

A third party ordered products from the Living Social website. The cost of the products was mistakenly charged to the data subject. On discovery of the error, the third party was able to access the data subjects personal data (name, email address etc.) from Living Social's website. The third party then contacted the data subject regarding what had happened. The Controller has refunded the data subject, but the data subject is not satisfied with their response as the Controller states that they do not believe a breach has occurred.

Findings

The LSA, after consulting with the controller, reached the conclusion that no breach had taken place since the controller only stores the last two digits of credit cards in its databases and uses payment tokens instead.

Decision

No violation.

Via email: [REDACTED]

Case Reference Number

Dear Sir/Madam,

Thank you for your recent correspondence, received 8 March 2019, with regard to the data protection complaint that has been raised with the ICO about how [REDACTED] has handled an information rights request submitted by [REDACTED].

Your organisation's response

In your reply, you have provided the ICO with a full chronology showing how this request has been dealt with.

Following [REDACTED]'s chaser emails of 5 January and 15 January 2019, you have stated that [REDACTED] liaised internally after having noted that [REDACTED] had yet to complete the necessary identification verification checks. [REDACTED] approached [REDACTED] via email on 23 January and later via email and phone on 31 January in order to pursue this matter further.

Unfortunately, it would seem that these emails were sent to [REDACTED]'s spam folder and were not seen for some time. [REDACTED] only confirmed his identity via phone on 6 February, more than one month after he was initially asked to do so.

Upon its receipt of this, your organisation escalated his request promptly and supplied him with an encrypted file containing his personal data via email on 15 February. A decryption password was sent separately to him on 28 February after he confirmed that he would be happy to receive this to the same email address.

Our view

I have considered the information available in relation to this data protection complaint and I am of the view that [REDACTED] has complied with its obligations under data protection law in this instance.

I believe it would have been better practice for your organisation to have given [REDACTED] the option of confirming his identity via email when [REDACTED] acknowledged his right of access request on 4 January, rather than directing him towards [REDACTED]. However, the ICO recognises that [REDACTED] proceeded to contact [REDACTED] again shortly after it received his second chaser email of 15 January and responded well within the statutory calendar-month timeframe once the required identity checks had been completed.

Consequently, we do not propose to take any further regulatory action on this matter.

Thank you for your assistance in addressing this data protection complaint. Should you wish to discuss this case any further, or require any clarification, please do not hesitate to contact me.

To correspond with me via email, you can forward any messages to our [casework@ico.org.uk](mailto:caserwork@ico.org.uk) email address with the above case reference in this format [REDACTED] in the subject line.

Yours faithfully,

Case Officer
Information Commissioner's Office
Direct dial number:

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice.

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	3 August 2019
LSA:	UK
CSAs:	AT, BE, BG, CY, CZ, DE, DK, EL, ES, FI, FR, HR, HU, IE, IT, NO, PL, PT, SE
Legal Reference:	Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12), Information to be provided (Articles 13-14), Right of access (Article 15)
Decision:	No violation
Key words:	Data subject rights, right of access

Summary of the Decision

Origin of the case

A French complainant asked the controller how to download all of his personal data and the controller went on with the necessary identification verification checks.

Findings

Upon receipt of the identity verification, the controller escalated the request promptly and supplied the data subject with an encrypted file containing his personal data via email, and subsequently with the decryption password. The initial delay in dealing with the matter was due to the fact that the emails from the controller had been sent to the data subject's spam folder.

Decision

The UK SA found that the controller complied with its obligations under the GDPR.

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

Background information

Date of final Decision	7 August 2019
LSA:	UK
CSAs:	AT
Legal Reference:	Right to erasure (Article 17)
Decision:	Violation identified; No regulatory action.
Key words:	Right to erasure, Marketing

Summary of the Decision

Origin of the case

The complainant stated that he asked the controller not to send him marketing emails, yet he continued to receive them.

Findings

The UK SA found that the controller did not comply with its data protection obligations.

The controller stated that the complainant sent his request to unsubscribe to a 'no-reply' email address, instead of using the 'unsubscribe' button. However, the email address was not clearly recognisable as a 'no-reply' email address.

Decision

The UK SA took note of the actions taken by the controller, including a change to its processes so that the email address from which marketing communications are sent is now monitored. No regulatory action was taken.

[REDACTED]

Via email: [REDACTED]

Case Reference Number [REDACTED]

Dear [REDACTED],

Thank you for your recent email correspondence of 14 May 2019 with regard to the data protection complaint that has been raised with the ICO relating to how [REDACTED] has processed [REDACTED]'s personal information.

Your organisation's response

In your reply, you advise that it is your organisation's understanding that [REDACTED] accidentally entered [REDACTED]'s phone number when he attempted to enter his own when making a [REDACTED] [REDACTED] website. As a result, [REDACTED] began to receive text message updates on [REDACTED] orders.

[REDACTED] first contacted [REDACTED] to raise concerns about this situation on 26 July and to ask for his phone number to be disassociated with [REDACTED] and his account. The Customer Care consultant he first spoke with said this would be looked into and proceeded to send a message to the [REDACTED] online fraud department. Unfortunately, this was not the correct team and it does not appear to be the case that the consultant ever forwarded the details of [REDACTED]'s request to the IT Service Desk as they were planning to.

Following this, [REDACTED] contacted [REDACTED] again on 21 September and then on 16 October 2018, advising that he was still continuing to receive text messages intended for [REDACTED]. [REDACTED] asked [REDACTED] for permission to amend the phone number on his account on 17 October 2018. However, he did not initially respond to this and a note was added to his account that no additional orders should be processed for him until correct contact details for him had been confirmed.

[REDACTED]'s phone number was removed from [REDACTED]'s account on 22 January 2019 when [REDACTED] attempted to submit another order. In the meantime, [REDACTED] had received more messages relating to [REDACTED]'s orders as [REDACTED] did not immediately inform its delivery courier, [REDACTED]. [REDACTED] that the accuracy of the associated phone number w question.

Our view

I have considered the information available to me in relation to this complaint and I am of the view that [REDACTED] has not complied with its obligations under data protection law in this instance.

Principle (d) of Article 5 of the General Data Protection Regulation ('GDPR') requires that the personal data processed by organisations should be accurate and, where necessary, kept up to date.

Given that your organisation did not take sufficient action to assure itself of the accuracy of personal data it was processing associated with [REDACTED]'s account when [REDACTED] first contacted you in July 2018, the ICO is not minded to believe [REDACTED] has met the requirements of the accuracy principle here.

Next steps

The ICO recognises that [REDACTED]'s standard operating policies and procedures do not seem to have initially followed by its staff in this case. We also note that you have provided the ICO with assurances that your organisation has reminded its Customer Care department about the importance of adhering to these policies and is in the process of conducting an internal review to see if any improvements can be made to them.

In light of this, we do not currently intend to take any regulatory action on this complaint. However, you should know that we keep a record of all the complaints raised with us about the way organisations process personal information. The information we gather from complaints may form the basis for action in the future where appropriate.

Our website contains significant advice and guidance about the processing of personal data and an organisation's obligations under data protection law, which may help to inform any decisions you make about the processing of personal data in the future.

Thank you for your assistance in addressing this data protection complaint. Should you wish to discuss this case any further, or require any clarification, please do not hesitate to contact me.

To correspond with me via email, you can forward any messages to our [casework@ico.org.uk](mailto:caserowk@ico.org.uk) email address with the above case reference in this format [REDACTED] in the subject line.

Yours sincerely,

Case Officer
Information Commissioner's Office
Direct dial number:

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice.

Summary Final Decision Art 60 Complaint

Failure to comply with the accuracy principle

Background information

Date of final decision:	3 August 2019
LSA:	UK
CSAs:	DK, FR, IT, SE
Legal Reference:	Principles relating to processing of personal data (Article 5), Right to rectification (Article 16), Right to object (Article 21)
Decision:	Failure to comply; no regulatory action.
Key words:	Accuracy, e-commerce, individual rights

Summary of the Decision

Origin of the case

A French complainant contacted the controller three times between July and October 2018 asking for his phone number to be disassociated from another person's account, as he had been receiving text message updates on orders he had never made.

Findings

Although the complainant's phone number was eventually removed from the other user's account, the UK SA found that the controller did not comply with its obligations under the GDPR as it did not take sufficient action to assure itself of the accuracy of the personal data it was processing. However, the UK SA recognised that the controller's standard operating policies and procedures were not followed by the staff in this case and that the controller provided assurances that it reminded its staff of the importance of adhering to such policies.

Decision

The UK SA decided not to take any regulatory action on this complaint.

Via email: [REDACTED]

Case Reference Number [REDACTED]

Dear [REDACTED],

I am writing further to my receipt of your email correspondence of 20 March 2019 with regard to the data protection complaint that has been raised with the ICO about how [REDACTED] has handled an information rights request submitted by [REDACTED].

Your organisation's response

In your initial response to the ICO of 18 March 2019, you provided the ICO with an account of how [REDACTED] has dealt with this request.

You supplied me with details of the data download export function that [REDACTED] users can access via their profiles and of how [REDACTED] used this function manually as the means of providing [REDACTED] with the disclosure of personal data he received on 6 September 2018. This export would have included all information connected to [REDACTED] on [REDACTED]'s databases, including all communications sent and received by the user through the [REDACTED]

Further to this, however, you have added in your email of 20 March that emails from staff team accounts could not have been included as part of this automated email functionality. Although [REDACTED] could have manually exported the emails [REDACTED] has exchanged with it, it did not do so as your organisation did not consider them to fall in scope of his request.

Our view

I have considered the information available to me in relation to this complaint and I am of the view that [REDACTED] has not complied with its obligations under data protection law in this instance.

[REDACTED] was explicit in his right of access request of 1 September that he was seeking all information [REDACTED] had stored about him. Given that he will be personally identifiable from any emails he will have exchanged directly with [REDACTED] staff, as well as from any internal emails in which he is discussed, I do not feel sufficiently assured that he has been provided with a comprehensive disclosure of everything to which he would have been entitled.

Action required

It is unclear to what extent [REDACTED] is still processing information from which [REDACTED] is personally identifiable that it has not already disclosed to him as part of its export download. However, in line with the above assessment, the ICO now requires your organisation to revisit the way it has handled this complaint, review any such personal data it still retains, and provide this to [REDACTED] as soon as possible.

I note in your response of 20 March that you appear to express concern about the potential for inappropriately disclosing the personal data of [REDACTED] staff here. On this point, I would indeed stress that [REDACTED] is only entitled to his own personal data in response to his right of access request, and not that of any third parties.

It is unlikely that this would be problematic regarding any emails he has exchanged with the [REDACTED] team directly, as he would have had sight of this personal data already. In the case of any internal emails, [REDACTED] should consider if it possible for these to be redacted of any such third-party personal data if the relevant staff members do not wish to give their consent for their data to be included.

For your information, the scope of [REDACTED]'s right of access request would only include personal data processed about him up to the date it was first made. Any new emails, for example, he sent your organisation after 1 September would not be covered.

Next steps

Our website contains significant advice and guidance about the processing of personal data and an organisation's obligations under data protection law, which may help to inform any decisions [REDACTED] makes about the processing of personal data in the future.

In addition to the guidance I have linked you to previously on determining what is and is not personal data, please find below a further link to more general information the ICO has published on an individual's right of access under the General Data Protection Regulation, which I hope is helpful.

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/>

In the absence of any evidence to support [REDACTED]'s claim that [REDACTED] disclosed third-party personal data to him when it initially responded to his request, this is not a matter we would seek to take forward at this time. It may be the case that we will need to contact you again if he is able to provide this evidence at a later stage.

More generally, you should know that we keep a record of all the complaints raised with us about the way organisations process personal information. The information we gather from complaints may form the basis for action in the future where appropriate.

Thank you for your assistance in addressing this data protection complaint. Should you wish to discuss this case any further, or require any clarification, please do not hesitate to contact me.

Yours sincerely,

Case Officer
Information Commissioner's Office
Direct dial number:

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice.

Summary Final Decision Art 60 Complaint

Failure to comply with the accuracy principle

Background information

Date of final decision:	3 August 2019
LSA:	UK
CSAs:	DK, FR, IT, SE
Legal Reference:	Principles relating to processing of personal data (Article 5), Right to rectification (Article 16), Right to object (Article 21)
Decision:	Failure to comply; No regulatory action.
Key words:	Accuracy, E-commerce, Individual rights

Summary of the Decision

Origin of the case

A French complainant contacted the controller three times between July and October 2018 asking for his phone number to be disassociated from another person's account, as he had been receiving text message updates on orders he had never made.

Findings

Although the complainant's phone number was eventually removed from the other user's account, the UK SA found that the controller did not comply with its obligations under the GDPR as it did not take sufficient action to assure itself of the accuracy of the personal data it was processing. However, the UK SA recognised that the controller's standard operating policies and procedures were not followed by the staff in this case and that the controller provided assurances that it reminded its staff of the importance of adhering to such policies.

Decision

The UK SA decided not to take any regulatory action on this complaint.

To be sent by email: [REDACTED]

1 October 2018

Case reference [REDACTED]

Dear [REDACTED],

Thank you for your response of 17 September 2018 regarding [REDACTED]'s data protection concern.

You have explained that [REDACTED] is required to retain customer information pursuant to regulation 40 and 41 of the Money Laundering, Terrorist Financing and Transfer of Funds Regulation 2017. You have explained that the Gambling Commission's Prevention of Money Laundering and Combating the Financing of Terrorism Guidance states that information should be retained for five years after the end of the business relationship. As a result, [REDACTED]'s information has been retained in line with guidance in order to comply with the legal obligations.

I have considered the information available in relation to this complaint and I am of the view that you have complied with your data protection obligations and we do not intend to take further action regarding the matter.

Thank you for your assistance with the matter.

Yours sincerely,

[REDACTED]
Lead Case Officer
Information Commissioner's Office
Direct dial number: [REDACTED]

Feedback about our service

If you are dissatisfied with the way your case has been handled, you can ask to have it reviewed. Please note that we do not usually accept a request for a case review more than three months after the closure of a case. For more information please refer to our website <https://ico.org.uk/concerns/complaints-and-compliments-about-us/>

ICO Statement



Information Commissioner's Office

You should be aware that the Information Commissioner often receives requests for copies of the letters we send and receive when dealing with casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

For information about what we do with personal data see our privacy notice at
www.ico.org.uk/privacy-notice

Summary Final Decision Art 60

Complaint

No infringement

Background information

Date of final decision: 11 September 2019

LSA: UK

CSAs: DE-Berlin

Legal Reference: Lawfulness of the processing (Article 6), Right to erasure (Article 17)

Decision: No infringement of the GDPR

Key words: Lawfulness of the processing, Right to erasure, Consumer protection, Anti-Money Laundering, Legal obligation

Summary of the Decision

Origin of the case

The complainant requested the deletion of her account on the controller's website. Her request was not granted by the controller. The complainant filed a complaint with the CSA.

Findings

According to UK anti-money laundering legislation, the controller was required to retain customer information for a period of five years after the end of the business relationship. The LSA found that the complainant's information had been retained in line with the controller's legal obligations.

Decision

As the controller complied with his data protection obligations, no further action towards it was taken by the LSA.

Dear [REDACTED]

The Information Commissioner's Office (ICO) is writing to you regarding the complaint from [REDACTED] about your handling of his request to have his personal data erased.

The ICO's role

Part of our role is to consider complaints from individuals who believe their data protection rights have been infringed. We want to improve the way organisations deal with the personal information they are responsible for.

Our view

I have considered the information available in relation to this complaint and I am of the view that you have complied with your data protection obligations.

This is because:

- J You responded to [REDACTED]'s request within a calendar month.
- J You explained your legal obligations, under the European Union's 4th Anti-Money Laundering Directive, to continue processing [REDACTED]'s personal data.

Specifically we note that in your organisation's privacy policy under [REDACTED] you state that you will retain a data subject's personal data for 5 years after a business relationship has ended.

It is understood that as the European Union's 4th Anti-Money Laundering Directive was transposed into UK law in the form of the Money Laundering Regulations 2017, it is also stated under [REDACTED]

[REDACTED]
[REDACTED]

And section [REDACTED] therefore states:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Therefore it is apparent that in your privacy policy you have aligned your refusal to delete the data subject personal data in line with Article 6(c) of the GDPR as you are required to continue to process this personal data due to a legal obligation.

However, in your response to [REDACTED]'s request you omitted details about [REDACTED]'s rights.

You did not explain to [REDACTED] that he has the right to complain to the relevant supervisory authority and his rights to seek a judicial review.

I note that your response provided a link to your privacy policy and this contains the contact details for the relevant supervisory authority. Unfortunately, this does not meet the obligations of providing the above information when responding to requests.

Please can you confirm that you are the appropriate contact for any future complaints. If so, please can you also provide your position.

We will keep a record of all the complaints raised with us about the way you process personal information. The information we gather from complaints may form the basis for action we may take in the future to ensure you meet your information rights obligations.

Yours sincerely

[REDACTED]
Case Officer
Information Commissioner's Office
Direct dial number: [REDACTED]

If you would like to provide us with feedback of any kind, please let me know

ICO Statement

You should be aware that the Information Commissioner often receives request for copies of the letters we send and receive when dealing with

casework. Not only are we obliged to deal with these in accordance with the access provisions of the data protection framework and the Freedom of Information Act 2000, it is in the public interest that we are open and transparent and accountable for the work that we do.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

Summary Final Decision Art 60 Complaint

No infringement of the GDPR

Background information

Date of final decision:	17 December 2019
LSA:	UK
CSAs:	AT, DE-Berlin, DE-Saarland, DE-Bavaria (Private sector), DK, ES, IT, NO, SE, SK
Legal Reference:	Lawfulness of the processing (Article 6), Right to erasure (Article 17)
Decision:	No infringement of the GDPR
Key words:	Right of erasure, Legal obligation, Anti-Money Laundering Directive

Summary of the Decision

Origin of the case

The complainant requested to have his personal data erased, but his request was rejected.

Findings

The LSA found that the controller replied to the complainant's erasure request within a month. In his reply, the controller explained that, in light of his legal obligation under the fourth Anti-Money Laundering Directive, he was obliged to retain the complainant's personal data for 5 years after the end of the business relationship.

However, the LSA found that the controller did not properly inform the complainant of his right to complain to the relevant supervisory authority and his right to seek a judicial review. In fact, the LSA considered that providing a link to the privacy policy containing the contact details of the relevant supervisory authority was not enough.

Decision

The LSA asked the controller to improve the information given to all data subjects, by introducing relevant information on the data subjects' rights to lodge complaint to an SA or seek for judicial review in the privacy policy.



By email only to: [REDACTED]

31 October 2019

Dear [REDACTED]

RE: Investigation of incident of 18 February 2019

I write to inform you that the ICO has now completed its investigation into the theft of personal data in relation to [REDACTED] customers.

In summary, it is my understanding an individual who had previously been employed by [REDACTED], and had legitimate access to [REDACTED] data held on the [REDACTED] portal exported unauthorised data. The [REDACTED], [REDACTED], [REDACTED], a [REDACTED] [REDACTED] were engaged on your behalf as data processors.

This case has been considered under the General Data Protection Regulation (the GDPR) due to the nature of the processing involved.

Based on the information you have provided, we have decided that regulatory action is not required in this case. The reasons for this are below.

Our consideration of this case

I have investigated whether [REDACTED] has complied with the requirements of data protection legislation.

In the course of my investigation I have noted that the [REDACTED] portal had a weak password and the ability to mass export data.

However, in the course of my investigation we have noted that the incident occurred due to a deliberate act of an ex-employee who used information that had been legitimately gained through his employment with [REDACTED] with the intention of extracting money from [REDACTED]

[REDACTED] had the relevant contracts in place with [REDACTED] and [REDACTED] as their data processors, which provided sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will

meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

There has been no damage or distress to any of the data subjects involved in this incident and you have not received any complaints as a result of the infringement.

We also welcome the remedial steps taken by [REDACTED] in light of this incident. In particular that you immediately took down the portal and following an investigation found vulnerabilities with 2 other portals which were not operating to the agreed standard and you also took those down. You contacted the affected data subjects informing them of the incident and told the data subjects to be vigilant in relation to phishing emails

Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action in this case.

Further Action Recommended

The Commissioner considers that [REDACTED] needs to take certain steps to improve compliance with GDPR. In particular:

1. Consider more regular reviews of any 3rd parties you engage to ensure they are meeting their contractual agreements in relation to compliance with data protection legislation including having appropriate technical and organisational measures, confidentiality and the processing of data only on your documented instructions to ensure the protection of rights of data subjects.
2. Consider how to improve password management with your providers, an area you have already identified.

Please note that if further information relating to this incident comes to light, or if any further incidents involving [REDACTED] are reported to us, we will revisit this matter, and enforcement action will be considered as a result.

Further information about compliance with the GDPR can be found at the following [link](#).

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[REDACTED]
Lead Case Officer
Investigations
Information Commissioner's Office
[REDACTED]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (<https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/>).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

Summary Final Decision Art 60

Personal data breach notification

No infringement of the GDPR

Background information

Date of final decision	10 January 2020
LSA:	UK
CSAs:	AT, BE, CY, CZ, DE, DK, EE, EL, ES, FI, FR, IE, IT, HU, LT, LU, LV, MT, NL, PL, PT, SE, SI, SK
Legal Reference:	Personal Data Breach (Articles 33 and 34)
Decision:	No infringement of the GDPR
Key words:	Data breach notification

Summary of the Decision

Origin of the case

The controller reported a data breach notification involving 643 of their customers in the EU. The former ex-employee accessed the customers data and exported them with the intention of extracting money from the controller.

Findings

In the course of its investigation, the LSA found that the controller had a relevant contract in place with the service provider, as a processor. The contract provided sufficient guarantees for their processing activities. There has been no damage or distress to any of the data subjects involved in this incident and the controller did not receive any complaints as a result of the infringement.

The controller implemented two remedial measures, by taking down the portals for which vulnerabilities were found, and by informing the data subjects about the data breach and possible phishing attempts.

Decision

Although no infringement to the GDPR was found, the LSA issued two recommendations to the controller. First, to implement more regular reviews of any third parties to ensure that they are meeting their contractual agreements in relation to compliance with data protection legislation

including having appropriate technical and organisational measures, confidentiality and the processing of data only on the documented instructions of the controller to ensure the protection of data subjects rights. Second, to improve password management with their service providers.

Summary Final Decision Art 60

Data breach notification

No sanction

EDPBI:UK:OSS:D:2020:100

Background information

Date of broadcast:	15 April 2020
LSA:	UK
CSAs:	BE, DE, EE, IE, EL, ES, FR, IT, HU, NL, PL, SI, SK, FI
Legal Reference:	Principles relating to processing of personal data (Article 5), Security of Processing (Article 32); Notification of a personal data breach to the supervisory authority (Article 33)
Decision:	No sanction
Key words:	Personal data breach, Remediation measures

Summary of the Decision

Origin of the case

On 21 August 2019, the controller reported a data breach to the LSA related to a payment infrastructure that enabled near real-time payments between bank accounts of the regional financial institutions.

The breach concerned an identifier linked by a customer to one of their bank accounts that can be provided to others to receive payments into the linked bank account) enumeration attack against a financial institution and their sponsor. The infrastructure included a feature that prompted an identifier lookup at the sponsor's addressing service feature whenever customers entered an identifier into the payee field in an online banking facility. Customers then would have displayed the identifier name registered with the introduced identifier, helping them to reduce the risk of payments to unintended recipients. The financial sponsor identified a larger than normal number of an identifier enquiries, and subsequent investigations led them to identify a vulnerability in their identifier lookup service.

Findings

The individual and organisation customer names, mobile phone numbers and the associated account numbers and BSB (Bank /State /Branch) number had been exposed by the breach. The LSA found that this was not a breach of the controller's systems, rather the processor's systems. The LSA also established that the exposed data could not be used to access a bank account by itself.

The breach affected thousands of individuals, a number of which were identified as customers of the controller and identified as being EU citizens.

The LSA found that the breach had caused low detriment to individual data subjects. The controller took steps to notify affected data subjects and heightened monitoring on the affected accounts to look for any signs of fraudulent activity, as well as offered them an independent enhanced fraud detection identification and cyber-monitoring service for free.

Decision

The LSA considered that whilst a data breach had occurred, and individual data subjects were affected, the breach did not meet the threshold for regulatory action due to the low number of affected EU data subjects and the post-incident actions taken by the controller to remediate the situation, which had reduced the risk of fraudulent activity on customers' accounts.

The LSA decided that no further action should be taken and closed the case.



521.11282 / 632.148
IMI: A56ID 55033, CR 64309, A60DD 71662

Final Decision

The complainant complained that in its privacy policy, the company had indicated a postal address in the USA as the only contact option, but not an e-mail address or a web form.

We first conducted a hearing to determine the lead supervisory authority. It was found that we are the lead supervisory authority. At the same time, the company announced that it had already decided in May 2018 to include the e-mail address in the privacy policy. The implementation had not taken place due to a human error. However, this was done immediately, so that the e-mail address compliance@mozilla.com and the link to a portal for enquiries from data subjects are now also integrated as a contact option. This has been checked by us.

Irrespective of the question as to whether there was a breach of data protection here, it no longer applies. We therefore see no reason to take any further action in this matter and conclude the matter.

Moreover the Austrian DPA has informed us that the complainant has withdrawn his complaint independently of this.

Berlin Commissioner for Data Protection and Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form for registering data protection complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please send an e-mail to:
mailbox@privacy.de

Fingerprint of our PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to Kochstraße / Bus number M29 and 248

Visit our Website

<https://privacy.de>

[REDACTED]
Georgenstraße 35
10117 Berlin
Germany

Sent by Independent Data Protection Center Schleswig-Holstein - Lander Commissioner for Data Protection

5 February 2020

J.No. 2019-7320-1396
Doc.no. 179147
Caseworker
[REDACTED]

Complaint about data breach

You have filed a complaint to The Independent Data Protection Center Schleswig-Holstein - Lander Commissioner for Data Protection regarding the controller Garnio ApS (hereinafter Hobbii ApS, as Garnio ApS changed its name on 8 April 2019). In accordance with Article 56 of the General Data Protection Regulation¹, the Danish Data Protection Agency (hereinafter the Danish DPA) has been designated as the leading supervisory authority of the case.

The Danish DPA understands that you have requested Hobbii ApS for access to your personal data in accordance with Article 15 of the General Data Protection Regulation, after which Hobbii ApS has sent you personal data regarding another person. The Danish DPA understands that you have contacted Hobbii ApS about the breach but the company has not reacted to your inquiry.

It is the understanding of the Danish DPA that you wish to complain about you having received personal data regarding another person.

1. Decision

The Danish DPA can inform you that according to Section 39(1) of the Danish Data Protection Act², the data subject or the data subject's representative may lodge a complaint with the competent supervisory authority concerning the processing of personal data concerning the data subject, as prescribed by Article 77 of the General Data Protection Regulation. This means that you are only entitled to complain about processing of personal data that concerns you.

After a review of your inquiry, the Danish DPA finds that you are not entitled to complain, as the processing of personal data is not related to you, but instead is related to the person of whom you received the data.

The Danish DPA has taken notice of the security problem and breach of personal data described and it will be included in the Danish DPAs ongoing considerations about which cases the Danish DPA will take during our own operations of audits.

The Danish Data Protection Agency
Carl Jacobsens Vej 35
2500 Valby
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk
[REDACTED]

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).

² Act No. 502 of 23 May 2018 – Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act)

Kind regards

Page 2 of 4



Appendix: Legal Basis

Extracts from Act No. 502 of 23 May 2018 – Act on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act)

Section 39(1) The data subject or the data subject's representative may lodge a complaint with the competent supervisory authority about the processing of data concerning the data subject, as prescribed by Article 77 of the General Data Protection Regulation.

(2) Decisions made by the supervisory authorities or their failure to consider a complaint from a data subject or their lack of reporting can be brought before the courts by the data subject or the data subject's representative to be considered under the rules of the administration of civil justice as set out in Article 78 of the General Data Protection Regulation.

(3) The data subject or the data subject's representative may bring issues of whether data controllers or data processors comply with this Act before the courts to be considered under the rules of the administration of civil justice as set out in Article 79 of the General Data Protection Regulation.

Extracts from 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).

Article 15(1) The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

(3) The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based

on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Page 4 of 4

(4) The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 77(1) Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

(2) The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.



Nr. 59/22.05.2024

Decision

Following the investigation performed at Hyllan Pharma SRL

The National Supervisory Authority for Personal Data Protection, with the headquarters in 28-30 G-ral Gheorghe Magheru Blvd., District 1, post code 010336, Bucharest, legally represented by Ancuța Gianina OPRE, President, **issues this decision against Hyllan Pharma SRL**, with the headquarters in Bucharest, 11A Turtură Street, 2nd Floor, sole registration code 21293833, registered with the Trade Registry under no. J40/4681/2007, legally represented by [REDACTED], [REDACTED], as director and [REDACTED], as data protection officer.

Considering the following:

I. Premises

The personal data security breach notifications received based on Article 33

Hyllan Pharma SRL notified a breach of the personal data security by filling in the form for the breach of the personal data security provided under 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), registered with the National Supervisory Authority for Personal Data Processing under no. 831/13.01.2023.

Hyllan Pharma SRL notified a breach of the personal data security by filling in the form for the breach of the personal data security provided under 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), registered with the National Supervisory Authority for Personal Data Processing under no. 894/16.01.2023.

Considering the above, ANSPDCP started an investigation at **Hyllan Pharma SRL**, through address no. 3770/23.02.2023.

Following the answer submitted through letters no. 4532 of 07.03.2023 and no. 4557 of 07.03.2023, the National Supervisory Authority for Personal Data Processing (hereinafter referred to as "ANSPDCP") acted as lead supervisory authority (LSA) in this case, given that this company has the main establishment in Romania, by introducing within the application "Internal Market Information System" a notification based on Article 56, registered under no. 561108, in order to inform the supervisory authorities from the other Member States of the European Union.

We present below a summary of the security incident and the results of the investigation performed by ANSPDCP in this case.

I. Description of the case:

Within the period 06.01.2023 – 10.01.2023, an illegal/unauthorized access to the data of a number of 24 clients of **HYLLAN PHARMA SRL** that bought online products via four websites was found. The infrastructure for the storage of the data is managed through the processor **ROMARG SRL**.

An unauthorized person accessed in an unauthorized way the database of **HYLLAN PHARMA SRL**, by adding an information structure from a folder that was collecting the card data of the data subjects. The collection was performed by the hacker by creating a fraudulent page that further

redirected to NETOPIA a part of the data, but also to the e-mail address **ahmadgenius@outlook.com**.

The compromised data are: **first name, last name, address, city, country, email, card number, card name, expiry date and CVC.**

From the preliminary assessment of the case, the controller concluded that the subject matter is a malware attack php.malware.fopo type. This malware type php.malware.fopo (php object injection) is a form of malware that is injected within the web applications written in php. and which spreads through the exploitation of the vulnerabilities from the web applications or through some phishing type attacks.

Within the personal data security breach notification form submitted by **Hyllan Pharma SRL**, under section "Technical and organisational measures taken (or following to be taken) by the controller", the following are mentioned:

1. The application of security patches: it is important to maintain the web applications and operating systems updated in order to benefit from the latest security patches. This can help to the closure of any known vulnerabilities that could be used by the attackers in order to exploit the system.
2. The use of a security software: the installation and use of a security software, such as a firewall or an antivirus can help to the prevention of the unauthorized access to the systems and to the detection and elimination of the malware software.
3. The implementation of data access rules: the implementation of the data access rules can help to the limitation of the access solely to the authorized persons and the limitation of the access to sensitive data.
4. The use of strong passwords and of the two-steps authentication: the use of a strong password and of a two-steps authentication method, such as a verification code provided via SMS, can help to the protection of the authentication data. Strong passwords should contain at least 8 characters, that shall contain uppercase letters, lowercase letters, numbers and special characters. The two-steps authentication adds an additional security level, because even if someone finds the passwords, he/she cannot access the account without the verification code.
5. The training of the employees: it is important to train the employees on the cybernetic risks and on how to avoid the accessing of dubious websites or the download of malware software.
6. The performance of penetration test regularly: the performance of penetration tests regularly can help to identify the vulnerabilities and take the necessary measures in order to remedy them.
7. The implementation of backup and disaster recovery rules: the implementation of backup and disaster recovery rules can help to the protection of the data in case of a security breach and their recovery in case of a data loss.
8. The use of an injection type protection solution against the attacks.
9. The implementation of a monitoring system: the implementation of a monitoring system can help to the detection and report of any unusual or suspect activities within the system. This system can monitor the network traffic, the users' activities, the events from the system and other security relevant activities. In case of detection of any suspect activities, the system can generate alerts in order to notify the security managers in order to take the necessary measures.

The number of natural data subjects affected by the incident is of **24**.

Under section "Possible consequences and adverse effects (risks) for the natural data subjects" from the security breach notification form submitted by **Hyllan Pharma SRL** it is mentioned that "the financial frauds (Lei 400) will be recovered with the help of the bank".

Also, within the same notification form, under section "Technical and organisational measures taken by the controller in order to mitigate the eventual negative effects", the following are mentioned:

1. The controller acknowledged in a short period of time the incident and ordered measures in order to handle it.
2. The data protection officer was contacted in order to bring to the knowledge and manage this risk.
3. The incident response team/commission met in the shortest possible time (11.01.2023) and analysed all relevant aspects, the priorities and steps to be further followed were established.
4. The reset of the vps access password was requested.
5. Within the ticket howx-9242-hjei the activation of the two-factor authentication was requested, that was performed on 10.01.2023 time 15:10.
6. The access passwords for all domains (passwords that were changed several weeks before, different for each domain and random generated) were changed.

It is mentioned that the information of all natural data subjects was performed, both by phone and by e-mail.

II. Handling proceedings performed by ANSPDCP

Through the letter no. 3770/23.02.2023, ANSPDCP requested additional information from **Hyllan Pharma SRL**, which responded through the letters no. 4532/07.03.2023 and no. 4557/07.03.2023 as it follows:

Q1: "the manner of manifestation of the cyberattack"

R1: *The cyberattack manifested as it follows: when placing an order, at the moment when the client chose as payment method – bank card and should have been redirected to the Netopia payment processor, he was actually redirected through an intermediary screen generated by the index.php file from the CC folder.*

In order for this redirection to the intermediary page to be performed, the hacker managed to amend also the page Netopia.php that contained the redirection to <https://secure.mobilpay.ro/> in the sense that it changed the code so as the client to get on the phishing page "public_html/CC/index.php".

Also, the cyber attack was type PHP injection, that is a form of cyberattack when an attacker uses a vulnerability within a web application ruling the PHP in order to execute their malicious code within the application. This can lead to the compromise of the data, to obtaining the unauthorized access to the resources of the application or to its complete take-over.

The PHP Injection type cyberattack manifested through the code injection: the attacker can insert a malicious code within a form or web interface running PHP. This code can be used in order to obtain access to the database of the application, in order to manage the data or to launch other attacks.

Q2: "the effects of the cyberattack on the hardware and software infrastructure, as well as on the electronic communication resources/channels used";

R2: *The effects of a PHP Injection type cyberattack can lead to the loss or compromise of the data, of the confidentiality, integrity or availability of the web application.*

Compromise of the data: The attacker can obtain access to the sensitive data, such as personal information, authentication details, financial information or other confidential information. This information can be used in unfavourable ways, such as fraud or identity theft.

Following the cyberattack **no effects** on the hardware and software infrastructure, as well as on the electronic communication resources/channels used by SC HYLLAN PHARMA SRL **were registered**. The breach was closed, and at this moment everything is functioning normally, without damages.

From a financial perspective, an unauthorized payment on behalf of a single data subject was performed. The blocking of the payment through bank was obtained and the money sum was fully recovered.

Q3: "the system logs on the access and/or download of the files/databases that are subject to this incident, with the mention of they were accessed and/or downloaded":

R3: We hereby provide you these system logs within the attachment (Annex 1).

Ip: 196.117.25.146

Q4: "the total number of natural data subjects affected by the security incident":

R4: 25 natural data subjects

Q5: "the content of the information for the natural data subjects affected by the security incident"

R5: We provide you the **Information letter** for the data subjects affected by the security incident within the attachment (Annex 2).

Q6: "the investigation report for the notified security incident, if there was an internal investigation or with experts within the domain":

R6: We hereby provide you the official request for the investigation of the phishing incident provided (on 10.01.2023) by Hyllan Pharma SRL to the service provider ROMARG SRL in attachment (Annex 3).

Q7: Considering those stated under point 16 from the notification form, namely the fact that also natural persons from other Member States were affected, we hereby request you to mention broken down by each Member State of the European Union the number of natural data subjects affected"

R7: Romania: 21 data subjects affected.

Italy: 4 data subjects affected

Q8: Considering the provisions of Article 24 and Recitals 75 and 76 from the Regulation (EU) 2016/679, with reference to point 11 from the notification, "eventual adverse consequences and effects (risks) for the natural data subjects", **we hereby request you to provide us if there is any evaluation procedure/methodology for the risk on the persons' rights and freedoms"**

R8: We hereby provide you in attachment (Annex 4-The evaluation of the risk corresponding to the incident for the personal data security), within **point II** – the identification of the risk factors and **point III**- the risks' matrix, the procedure/methodology for the evaluation of the risk on the persons' rights and freedoms in the case of that incident.

The following technical measures were taken:

- The access data of the users managing the pages were changed
- The two-steps authentication with password available for two minutes was implemented
- We constantly follow the authentication log, to see if authentications at unusual hours appear
- We created a soft that monitors the status of the system by verifying two consecutive statuses so, if there are extra files or files are erased or the dimension of a file is amended, we have the alert on e-mail

Q9: Considering the provisions of Article 24 and Recitals 75 and 76 of Regulation (EU) 2016/679, by reference to point 11 from the notification "eventual consequences and adverse effects (risks) for the natural data subjects", **we request you to provide us with an evaluation regarding the risk for the persons' rights and freedoms, that would encompass inclusively the fitting into a risk degree (low, medium, high)**

R9: We provide you attached (Annex 4) the **Assessment of the risk** corresponding to the incident for the personal data security (performed on 12.01.2023)

Q10: "The service agreement concluded by **HYLLAN PHARMA SRL** with the processor **ROMARG SRL**"

R10: We hereby provide you attached the Service agreement concluded by HYLLAN PHARMA SRL with the processor ROMARG SRL (Annex 5).

III. Information of the concerned supervisory authorities within IMI

On 27.09.2023, through the IMI application, the other supervisory authorities were informed (specifically the authority from Italy), within a LSA and CSA identification procedure regarding the security incident (based on Article 56 of the GDPR), as well as in relation to the intention of our institution to act as lead supervisory authority, registered under no. 561108, with response deadline until 29.12.2023.

Until the date of this decision, the following supervisory authorities declared themselves as CSA:

- The supervisory authority from Italy;
- The supervisory authority from Spain (with the mention: "according to the information available, there are no sufficient elements to ensure that the data subjects from Spain have been affected, so ES SA is not CSA. However, in case additional proofs according to which the natural data subjects from Spain are affected are identified, ES SA would be CSA");

On 15.04.2024, the Italian supervisory authority was informed, through the IMI application, about the draft Decision, without making observations/comments on the ANSPDCP proposal.

IV. Conclusions:

From the investigation performed by ANSPDCPD through letters no. 3770/23.02.2023 and from the responses of **Hyllan Pharma SRL** no. 4532/07.03.2023 and no. 4557/07.03.2023, the following resulted:

- within 06.01.2023 – 10.01.2023 an illegal/unauthorized access to the personal data of a number of 24 natural data subjects (clients) of Hyllan Pharma SRL, that acquired online products through 4 websites (profecund.it, profecund.ro, normens.ro, steablock.ro) was found. The infrastructure for the storage of the data is managed by the processor "Romarg SRL";
- a hacker accessed unauthorized the database of Hyllan Pharma, by adding an information structure within a file that was collecting the card data of the data subjects;
- the collection was performed by the hacker by creating a fraudulent page that was redirecting to Netopia the data on one hand, but also to the e-mail address ahmadgeniius@outlook.com;
- the possibly compromised personal data, in the sense that the attacker could obtain access to personal information, authentication details, financial information or other confidential information are: first name, last name, address, city, country, email, credit card number, name from the credit card, expiry date and CVC;
- the number of affected persons is of 24 natural data subjects;
- the cyberattack was a malware attack type "**php.malware.fopo**", being a form of malware that is injected within the web applications written in PHP.
- as immediate effects of a PHP.Malware.FOPO (PHP Object Injection) attack may vary depending on the purpose and abilities of the attacker, but may include: unauthorized access to the application's data, information theft, distribution of additional malware;
- as technical and organisational measures were applied by the controller, both before and after the incident, the following:
 - a) the ordering of measures for the handling of the attack;
 - b) the contacting of the Data Protection Officer;
 - c) the reunion of the incidents' response team/commission in the shortest time and there have been analysed the relevant aspects and the establishment of the priorities and steps to be followed;
 - d) the reset of the VPS access password;
 - e) the activation of Two-Factor-Authentication;
 - f) the change of all access passwords for all web domains (passwords that were changed with several weeks before, different for each domain and randomly generated).

- g) The opening of a criminal action from the perspective of committing the crime of illegal access to data provided under Article 360 paragraph (3) from the Criminal Code corroborated with Article 364 – Illegal transfer of data;
- h) The notification of the National Cyber Security Directorate in order to support the research and to offer the recommendations necessary for the reduction of the risks corresponding to the incident;
- i) The creation of a software that monitors the status of the system by verifying two consecutive statuses so as if there are extra files or files are erased or the dimension of a file is amended to provide an alarm on the e-mail.

V. Analysis according to the criteria provided under Article 83 GDPR

The conclusions resulting following the analysis of the security incident according to the criteria from Article 83 of the GDPR:

- a) the nature, gravity and duration of the infringement, the scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them:
 - 25 data subjects (24 clients and 1 employee)
 - The systems of Hyllan Pharma SRL were subject to a PHP Injection cyberattack following which the hacker modified the Netopia.php page that contained the redirection to <https://secure.mobilpay.ro/> in the sense that it changed the code so as the client to get on the phising page "public_html/CC/index.php" when he was choosing the payment method – credit card;
 - No complaints were submitted by the data subjects affected by the security incident notified by Hyllan Pharma SRL, therefore no damages incurred by the latter were able to be identified
- b) the intentional or negligent character of the infringement
 - "php.malware.fopo" malware cyberattack
- c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
 - the data subjects affected by the incident were informed through the electronic mail (email) inclusively in relation to the security of the credit cards in order to avoid potential damages
 - the transactions were blocked and the financial frauds were recovered (Lei 400, the equivalent of Eur 800);
 - an evaluation on the risk for the rights and freedoms of the data subjects was performed;
 - after the incident took place additional technical and organisational measures were taken.
- d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
 - immediately ordered measures for handling the attack;
 - summoned the incident response team/commission in the shortest time and analyzed the relevant aspects and established the priorities and steps to be followed;
 - d) resetting the VPS access password;
 - e) the activation of Two-Factor-Authentication;
 - f) the change of all access passwords for all web domains (passwords that were changed with several weeks before, different for each domain and generated randomly)
 - g) the opening of a criminal action for the crime of illegal access to data provided under Article 360 paragraph (3) from the Criminal Code corroborated with art. 364 Illegal transfer of data;
 - h) the notification of the National Directorate for Cyber-Security in order to support the research and offer the necessary recommendations for the reduction of the risks corresponding to the incident;
 - i) the creation of a soft that monitors the status of the system by verifying two consecutive statuses so if additional files appear or files are deleted or the size of a file is changed to submit an alarm on e-mail.
- e) any relevant previous infringements by the controller or processor;

- no previous breaches were identified
- f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement:
- the controller **notified the security incident within the deadline provided under the GDPR and communicated to ANSPDCP all information requested within the investigation performed;**
- g) the categories of personal data affected by the infringement:
 - first name, last name, city, country, email, credit card number, name from the credit card, expiry date and CVC;
 - according to the system's logs regarding the access and/or download of the files/databases it resulted that **the personal data have not been downloaded or accessed;**
- h) the manner in which the infringement was brought to the knowledge of the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement:
 - the controller **notified the security incident within the deadline provided under the GDPR and communicated to ANSPDCP all the information requested within the investigation performed**
- i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures:
 - no measures were previously applied
- j) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement:
 - the security incident took place following a malware cyberattack

Considering the conclusions resulting from the investigation performed at Hyllan Pharma SRL, the technical and organisational measures taken by the controller, the fact that the data subjects affected were informed through electronic letter, as well as the fact that from the verification of the ANSPDCP's registrations, it resulted that based on the GDPR there have not been applied sanctions against Hyllan Pharma SRL, we consider that the measures adopted by the controller in the sense of Article 34 paragraph (3) letter b) of the GDPR are sufficient, which is why **we consider that in this case the application of a sanction is not required.**

President,

Ancuța Gianina OPRE

Summary Final Decision Art 60

Complaint

Reprimand to controller, Temporary limitation on data processing

EDPBI:RO:OSS:D:2020:163

Background information

Date of final decision:	8 October 2020
Date of broadcast:	10 December 2020
LSA:	RO
CSAs:	DE, DK, ES, FR
Controller:	Microstockr SRL
Legal Reference:	Right to erasure (Article 17), Conditions for consent (Article 7)
Decision:	Reprimand to controller, Temporary limitation on data processing
Key words:	Right to erasure, consent, cookies, anonymisation

Summary of the Decision

Origin of the case

The complainant requested the erasure of his account on the website of the controller, which the controller denied. The controller alleged that this was the second time the complainant requested to have his account deleted, after the first request to delete his account was already granted by the controller. Following its investigation, the LSA also assessed the legality of processing of personal data collected by the controller on the controller's website.

Findings

The LSA found that the use of cookies by the controller was not in accordance with the conditions for consent under Art. 6.1 (a) and Art. 7 GDPR.

Decision

The LSA issued a reprimand and a temporary limitation for the use of cookies until the correct implementation of a method for obtaining the prior explicit and informed consent of the users. In addition, the LSA required the controller to implement a method of anonymisation to prevent the risk of re-identification of persons whose personal data are subject to this procedure and to establish a

limited duration (less than 3 years) for the storage of data related to inactive accounts and to apply, in their case, the anonymisation method used also in the case of active accounts.



**ANSPDCP. Registrul Evidenta Decizii Avize
Recomandari.0000068.08-10-2020**

Decision

following the investigation performed Microstockr SRL

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), having the premises at 28-30 Gen. Gheorghe Magheru Blvd., 1st District, PO 010336, Bucharest, legally represented by [REDACTED], President issues this decision against Microstockr SRL, with its headquarters in 16 Lunii Street, Block L11, Scale 2, Floor 3, Apartment 24, Cluj-Napoca Municipality, Cluj County, registered at the Trade Register under no. J12/124/2017, fiscal identification code 36929310, represented by Mr. [REDACTED]

Considering the following:

I. Premise

1. Intimation pursuant to Article 56 of GDPR

By the application no. 66211/2019 introduced in IMI pursuant to Article 56 of 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 – hereinafter "GDPR"), the data protection authority from the Nordrhein-Westfalen Land (Germany) requested the opinion of ANSPDCP which it considers to be the lead authority (as the only office of the complained data controller is based on the Romanian territory) in the following case:

Mr. [REDACTED] (according to the annexes sent to the request 66211) complained that the right of erasure of his data related to an account created for the use of an application made available by Microstockr SRL (based in Cluj-Napoca) was not respected. From the response sent by the controller including to the German authority, it is noted that the data and the account of the petitioner were initially deleted (after the free of charge use for one month of the application, for verifying its functionality), but subsequently he created a new account based on the same credentials and used the app again for a month free of charge. Against this situation, the controller decided not to delete his data in order to prevent the creation of a new account and the re-use of the application free of charge. Microstockr SRL provides an application for photographers to track the remuneration received from the various agencies where they have created accounts.

The German authority considers that many EU users use this application and, as such, the issue of data deletion seems to be a problem with cross-border impact.

Following the initiation of the procedure in IMI, the authorities from France, Denmark and Spain declared themselves to be concerned authorities as the processing would affect or could substantially affect data subjects in their country.

2. Responses of other supervisory authorities in IMI

A. Within the notification pursuant to Article 56 in IMI under no. 66211 (opened on the 6th of May 2019), the authorities from France, Denmark, Spain and Nordrhein-Westfalen Land of Germany declared to be concerned supervisory authorities.

Following the acceptance of the proposal to be the lead authority in this case, ANSPDCP opened the case of informal consultation in IMI under no. 71416, on the 9th of July 2019, pursuant to Article 60, specifying that the Romanian authority initiated an investigation and asking the other EU authorities for relevant information, if they consider themselves to be concerned supervisory authorities, with further explanations (e.g. how many complaints against Microstockr SRL were received, on what subject etc.). In this case from IMI, the authorities of the following stated declared to be concerned authorities: Germany, Nordrhein-Westfalen Land (received one complaint), Czech Republic, France, Denmark, Sweden, Spain. The authorities from France and Denmark further explained that they noticed that there is a Microstockr mobile app in the Google Play Store and in App Store in French and English, explanation also given by the authorities from Sweden and Spain. Apart from the German authority, no other authority has stated that it had received any complaint against Microstockr SRL.

B. Following the introduction of a first draft of the decision issued by ANSPDCP in IMI (Article 60 118884), the authorities from France, Denmark, Spain (comments made in IMI) and Land of North Rhine-Westphalia (comments sent by e-mail) sent a series of comments on the legal basis chosen by the controller for not to delete the personal data in order to prevent fraud, on the method for obtaining the prior consent on the use of cookies, on prior information on the purposes of the processing, on the use of MD5 hash method that presents the risk of re-identification of the data subjects, on the data that are subject to the MD5 hash procedure, on the destination of the inactive accounts.

3. Investigation at Microstockr SRL

ANSPDCP sent two investigation letters to Microstockr SRL: letter no. 15899 of the 9th of July 2019; letter no. 21475 of the 24th of September 2019 (sent by regular mail and by electronic mail).

Microstockr SRL replied to the two letters with: letter no. 20452 of the 10th of September 2019 (received through the court executor) and no. 20666 of the 12th of September 2019 (by electronic mail); letter no. 22258 of the 7th of October 2019 (sent by electronic mail) and no. 22297 of the 7th of October 2019 (sent by regular mail).

In order to clarify the issues raised by the authorities from France, Denmark, Spain and the Land of North Rhine-Westphalia, ANSPDCP sent the letter registered under no. 11372 of the 28th of May 2020, to which Microstockr SRL responded with the letter registered under no. 11954 of the 9th of June 2020.

4. Minutes of the finding

Following the investigation, the minutes of the finding no. 17062 of the 24th of August 2020 was concluded, in which the following conclusions were held:

1. Microstockr application centralises/aggregates sales from various agencies, through which they sell photos of the contributors, in one place; in this way, it saves the user time and gives him/her an overview of his/her own portfolio;

2. when creating a new account, the following user data is collected: first name, last name, email and password of the Microstockr account. When the same user becomes a subscriber, the address, city, country, postal code and VAT code for invoicing are additionally collected (the VAT code is optional and is collected only in case of companies); this information is stored on the server, in the database of Microstockr SRL;
3. the representative of Microstockr SRL stated that it processes the personal data of some persons (555 active clients) from 75 states (including all the EU states), thus fulfilling the conditions of cross-border data processing within the meaning of Article 4 point 23 letter b) of Regulation (EU) 679/2016 ("or processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State");
4. the personal data corresponding to each account are kept legible as long as the accounts are active; in case of deleted accounts, the personal data is kept in encrypted form during the existence of the application on the market, after which they will be deleted. An account is considered inactive after a period of 3 years from the last use. In the case of deleted accounts, the personal data is anonymised by using the hash functions by the MD5 encryption method;
5. currently, "the Microstockr accounts are deleted by contacting support@microstockr.com and, after the request, the deletion operation is performed manually. This applied to all accounts, both those in the trial period and those with a subscription." The representative of Microstockr SRL said that in the near future is planned to add a "Delete Account" button within the application that will allow the deletion automatically. When an account is deleted, the client's personal data are stored in encrypted form in the database, as a hash generated by MD5 encryption method. This data can no longer be decrypted and the person can no longer be identified. "A hash is from an account that has the trial period attached. When a user creates a new account with the same email, the hash of the new email is compared to each deleted account hash and, if they are identical, the deleted account is reactivated, overwriting the hashes with the data entered by the user, without benefiting once more of the free of charge month. The representative of Microstockr SRL said that keeping there personal data in the hash form is the mechanism by which the controller is protected from the exploitation of the trial period. If the hashes do not match, a new account is created that will benefit from a "free trial" (one month trial period);
6. according to the statements of the representative of Microstockr SRL, the case of Mr. [REDACTED] (Germany) was an unique one in terms of exercising the right to erasure of data. The data collected in his case were first name, last name, Microstockr email account and Microstockr password. The account was initially created between 27 January and 27 February 2018 (the exact date is not known, the information being subsequently deleted). Following the request of the 25th of March 2018 to delete the account, Mr. [REDACTED] account was marked as deleted, but his data was kept to prevent fraud. On the 4th of April 2018 an email conversation with Mr. [REDACTED] takes place informing him that the email address and the agency account associated with the Microstockr Pro as a measure to prevent the attempts to create again a new account free of charge. On the 27th of May 2018, Mr. [REDACTED], invoking the right to erasure of data provided by GDPR, requests the deletion of all Microstockr accounts associated with [REDACTED]. To this request, Microstockr SRL responds on the 28th of May 2018 that it has deleted all personal data and saved the usernames associated to his account as hash MD5 in order to prevent the creation of a new free account. On the 30th of May 2018, Mr. [REDACTED] creates a new free account, used until the 30th of June 2018, a possible operation since at that time Microstockr SRL had not yet implemented (for logistical reasons) the mechanism for verifying the creation of new accounts based on the same data. On the 1st of July 2018, Mr. [REDACTED] requests the deletion of the data associated with the account [REDACTED], a request repeated on the 16th of July 2018. Microstockr SRL informs the petitioner on the 2nd of July 2018 and on the 26th of July 2018 that it refuses to "erase the data". Mr. [REDACTED] again request information regarding the erasure of his accounts on the 15th of February 2019 and Microstockr SRL replies to him on the 19th of February 2019 that it has deleted all "non-vital" information regarding the petitioner. Microstockr SRL

implemented the hash verification mechanism on the 2nd of July 2018, date when the second account created by Mr. ██████████ was anonymised an the first account was completely deleted;

7. by accessing the website microstockr.com it is allowed to install cookies belonging to third parties such as: _ga, _gat, _gid (Google Analytics cookies that allow the tracking of the browsing behaviour of the users on the website and helps to improve the use of this website), _fbp (cookie used by Facebook for the purpose of "Targeting/Advertising"), some of them having a validity period longer than that related to a session of use of the website;
8. although a banner containing a text (exclusively in English) regarding the use of cookies ("We use cookies to operate our website as expected and for performance and analytics purposes. By using our website, you agree to our use of cookies as described in our Cookie Policy") and a button for accepting them ("I accept") are available on the first page, it is noted that, after browsing various pages of the website, the cookies are installed on the user's terminal device, although it does not access beforehand actively the button to accept the conditions regarding the use of cookies. Such way of obtaining the consent does not correspond to the provisions of Article 6 paragraph (1) of Regulation (EU) 2016/679, related to the definition given to the consent in Article 4 point 11 of the same act: "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". As such, they are not cumulatively fulfilled conditions imposed by Article 4 paragraph (5) of Law no. 506/2004 which provided the following:

"(5) The storage of information or gaining access to the information stored in the terminal equipment of a subscriber or user is allowed only if the following conditions are cumulatively fulfilled:

- a) the subscriber or user concerned has expressed his/her consent;
- b) the subscriber or user concerned was provided, prior to the express consent, accordance with Article 12 of Law no. 677/2001, modified and amended, with clear and comprehensive information that:
 - (i) are to be presented in an easy-to-understand language and easily accessible to the subscriber or user;
 - (ii) are to include mentions about the purpose of the processing of information stored by the subscriber or user or of information to which he/she has access.

If the provider allows third parties to store or to have access to information stored in the subscriber's or user's terminal equipment, the information pursuant to points (i) and (ii) shall include the general purpose of the processing of this information by the third party and how the subscriber or user may use the settings of the Internet browsing application or other similar technologies to delete the stored information or to deny third party access to this information."

9. from the letter no. 22297 of the 7th of October 2019 it follows that the information collected using the cookies used by Google Analytics are automatically transmitted to Google, being "out of control" of Microstockr SRL;
10. regarding the _fbp cookie file, the representative of Microstockr SRL stated that it is generated by Facebook Pixel and uses it in the marketing campaigns carried out on the social network, without the noting that an express consent of the users of the microstockr.com website is requested in view of using this type of file.

No previous situation regarding the application of a administrative sanction/corrective measures against Microstockr SRL was identified in the ANSPDCP's records.

The deed found:

On the date of concluding this minute, it was found that Microstockr SRL, with the identification data mentioned on the first page of the minutes, did not present evidence on obtaining the unequivocal consent of the users of the website belonging to microstockr.com before allowing the storage of information or gaining access to the information stored on the user's terminal equipment, by using cookies having as purpose obtaining analytical and marketing information, thus infringing the

provisions of Article 6 paragraph (1) letter a) and Article 7 of Regulation (EU) 2016/679, by reference to the definition provided by Article 4 point 11 of this act.

This deed constitutes a contravention pursuant to Article 12 of Law no. 190/2018, by reference to the provisions listed in Article 83 paragraph (5) letter a) of Regulation (EU) 2016/679.

The sanction imposed:

Since in this case Microstockr SRL carries out a cross-border processing, it becomes applicable the provisions of Article 60 of Regulation (EU) 2016/679, as well as of Article 16 paragraphs (3), (5), (6), (7) of Law no. 102/2005, republished, which provide for the application of sanctions/corrective measures by decision of the president of ANSPDCP, which is based on the minutes of finding and on the report of the investigative personnel.

II. RECITALS:

Having regard to the findings from the investigations carried out at Microstockr SRL, the information and comments sent by the other concerned supervisory authorities in IMI (cases Article 56 – no. 66211, Article 60 Informal consultation no. 71416, Article 60 Draft decision no. 118884),

The additional information sent by Microstockr SRL with the letter no. 11954 of the 9th of June 2020, according to which:

- "the reason why the data have not been completely deleted, but are kept in pseudonymous form, is the prevention of fraud of our service and the unlimited exploitation of the Trial Period"; in this sense, the controller invoked Article 6 paragraph (1) letters a), b) and f) of the GDPR as a legal basis for the processing;
- the reasons why the controller continues to process pseudonymised data are the follows:

"- The malicious intent on the part of the user. It has abused our system repeatedly, as we have shown in our previous replies. In short, Mr. [REDACTED], after requesting the deletion of the original account, created a new account to benefit once again from the Trial Period, thus violating the Terms and Conditions of our service;

- The risk of company bankruptcy. If we do not take any action against this type of behaviour, our service could be defrauded indefinitely. This would reduce the company's revenues and the possibility of developments and maintenance and, in the long run, would lead to the closure of the service and its withdrawal from the market. We mention that this mode of operation, widely used, would close any online service based on subscription;

- We respect the fundamental rights of the user. We do not infringe any of his fundamental rights, as required by Article 6, paragraph (1) letter f), cited above; their observance allowing the further processing of personal data in accordance with the legitimate interests of our service. This data is not used for any other purpose such as marketing or profiling and is not transmitted to another processor or third party. They are only used to verify a potential fraud."

- the information of the data subjects is made as follows:

"To create a Microstockr account each user shall agree with the Terms and Conditions and the Privacy Policy of our company. This involves reading these provisions and is done by checking a box on the Sign Up, representing the user's consent to the processing of personal data. It is an Internet standard used by most online services."

Under Section "Terms and Conditions" (<https://microstockr.com/terms-conditions>) it is mentioned:

"You may not and you agree not to enable others to [...] try to extend the Trial Period [...]. We reserve the right to terminate any account which is responsible for such violations. Any microstock agency account associated with it will be prevented from further use in the Application."

Under Section "Privacy Policy" (<https://microstockr.com/privacy-policy>) it is mentioned:

"We also store your agency usernames and emails associated with the Application email to prevent them being used on a new Application account and exploit the free trial period indefinitely. In case of account deletion this data will be anonymized by hashing."

- the procedure for anonymising the data relating to the accounts is as follows:

- " a. The deletion request is registered and a case is opened
- b. The data protection officer (DPO) takes over the request Ofiterul
- c. The entry in the database is identified
- d. The username fields in both tables containing personal data of the user are pseudonymised by hash method
- e. Personal data fields password, first_name, last_name, address, postcode, city, country, country_id, company_name, vat_number, customer_id, plan_id, subscription_id, subscription_status, beta are completely deleted and take the value NULL
- f. The user is informed by the DPO that his account has been deleted and the case is closed"

- the destination of the inactive accounts was explained as follows:

"Inactive accounts remain stored in our database during the operation of the service, aspect which is mentioned in the Privacy Policy:

'We also store, for the duration our service is active, your agency usernames and emails associated with the Application email to prevent them being used on a new Application account and exploit the free trial period indefinitely.'

When an user requests the deletion of his account, we initiate the "anonymisation procedure" described above.

The "Privacy Policy" also mentions the following:

"An account is deemed inactive if no activity is registered in the past three years. The personal data associated with such an account will still be stored on our servers, for the duration of our service, to prevent exploiting the free trial period, as detailed above."

Recital (47) in the preamble of the GDPR, according to which the processing of data for preventing fraud constitutes a legitimate interest of the data controller,

The storage of data related to inactive accounts during the functioning of the service, for a period that does not correspond to the purposes of the processing, pursuant to Article 5 paragraph (1) letter e) of the GDPR,

The use of pseudonymisation method (hash MD5) which is considered to present some risks of re-identifying the data subjects (see in this respect the Opinion of WP29 no. 5/2014 on the anonymisation techniques, WP 216 of the 10th of April 2014, p. 21-22),

Given: the number of data subjects (55 active Microstockr clients); the receipt of a single complaint from a single data subject (from Germany); the reasons presented by the controller to legitimately justify the retention in encrypted form (MD5 hash) of the personal data associated with a deleted account in order to avoid the creation of a new free account (only valid for one month); information of the data subjects available on the website; the remedied made by the controller during the investigation; the use of cookies belonging to third parties (Google, Facebook) through the website microstockr.com for analytical and marketing purposes, without first obtaining the consent of the users of the website,

The unfounded character of Mr. ██████████'s complaint, under the aspect of requesting the erasure of his personal data,

Having regard to the provisions of Article 5 paragraph (1) letter e), Article 6 paragraph (1) and of Article 7 of GDPR, related to the definition from Article 4 point 11 of GDPR regarding the conditions under which the processing of personal data can take place based on the consent of the data subjects, as well as of Article 4 paragraph (5) of Law no. 506/2004 regarding the legal conditions in which it is allowed to store information or to gain access to the information stored on the terminal equipment of a subscriber or user, as well as of Article 32 of the GDPR,

Taking into account the case law of the Court of Justice of the European Union, in particular, the Judgement of 29th of July 2019 in Case C-40/17 ("Fashion ID") regarding the obligation of the administration of a website to obtain the consent of its visitors and to ensure the information of the data subjects with respect to the processing of personal data, in case of insertion of a social module

that allows the visitor browser to request content from the provider of this module, but also the one resulting from the Decision of the 1st of October 2019 in case C-673/17 ("Planet49"), regarding the obligation to comply with Article 5 paragraph (3) of Directive 2002/58/EC (transposed in Romania by Law no. 506/2004), in the sense of enabling the user to express his/her free consent, after being provided with clear and complete information, in relation to the storage of information or to the acquisition of access to information already stored in a user's terminal equipments by means of cookies, consent which has the same meaning as the consent referred to in Article 6 paragraph (1) letter a) and Article 4 point 11 of the GDPR, expressed through an active behaviour, a manifestation of the "free, specific, informed and unambiguous" will of the data subject, in the form of a statement or an "unequivocal action" (see, for example, paragraphs 46, 50, 54 and 61 of this judgement),

Pursuant to Articles 14, 15 and 16 of Law no. 102/2005, republished, of Article 12 of Law no. 190/2018 related to Article 83 paragraph (2) and to the provisions listed in Article 83 paragraph (5) letter a) of Regulation (EU) 2016/679, corroborated with the provisions of Article 58 paragraph (2) letters b), d) and f), as well as of Article 60 of Regulation (EU) 2016/679, related to the provisions of Articles 24, 25 and 26 of the Procedure for carrying out investigations, approved by the Decision of the president of ANSPDCP no. 161/2018,

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

ORDERS

the following measures against Microstockr SRL:

1. Issuing a reprimand for the fact ascertained through the minutes no. 17062 of the 24th of August 2020, based on Article 58 paragraph (2) letter b) of Regulation (EU) 2016/679;
2. Imposing the corrective measure provided by Article 58 paragraph (2) letter f) of Regulation (EU) 2016/679 to temporary limit the use of cookies belonging to Google and Facebook, until the correct implementation of a method for obtaining the prior express and informed consent of the users of the website microstockr.com for this purpose, pursuant to Article 6 paragraph (1) letter a) and Article 7 of Regulation (EU) 2016/679, by reference to the definition provided by Article 4 point 11 of this act and Article 4 paragraph (5) of Law no. 506/2004;
3. Imposing the corrective measure provided by Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to implement a method of anonymisation to prevent the risk of re-identification of persons whose personal data are subject to this procedure, pursuant to Article 32 of Regulation (EU) 2016/679 – deadline: 20 working days from the date of communication of this decision;
4. Imposing the corrective measure provided by Article 58 paragraph (2) letter d) of Regulation (EU) 2016/679 to establish a limited duration (less than 3 years) for the storage of data related to inactive accounts and to apply, in their case, the anonymisation method used also in the case of active accounts, at the expiry of the period mentioned previously, in order to comply with the principle provided by Article 5 paragraph (1) letter e) of Regulation (EU) 2016/679 – deadline: 10 working days from the date of communication of this decision.

Microstockr SRL shall communicate to ANSPDCP the measures adopted for the implementation of the corrective measures within 45 days from the communication of this decision.

This decision was subject to the procedure provided for in Chapter VII of Regulation (EU) 2016/679, being sent for approval to all concerned supervisory authorities.

This decision, together with the minute no. 17062 of the 24th of August 2020 shall be communicated to Microstockr SRL that has the right to challenge them pursuant to Article 17 of Law no. 102/2005:

"Article 17

(1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative contentious section of the competent court, within 15 days from handing, respectively from communication. The decision resolving the appeal can be appealed only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.

(2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued.

(3)The deadline of payment of the fine is 15 days from the date of handing, respectively from the date of communication of the minutes of finding/sanctioning or of the decision of the president of the National Supervisory Authority."

President,





**ANSPDCP. Registrul Evidenta Decizii Avize
Recomandari.0000031.30-08-2021**

Decision

**following the investigation carried out at
Cylex Tehnologia Informației Internațional Societate în Nume Colectiv**

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, having the premises at 28-30 Gen. Gheorghe Magheru Blvd., 1st District, PO 010336, Bucharest, legally represented by Mrs. [REDACTED], President **issues this decision against Cylex Tehnologia Informației Internațional Societate în Nume Colectiv**, with the premises in Palota village, Sîntandrei Commune, no. 119/A, Bihor County, Unique registration code 26332771, registered at the Trade Register Office under no. J5/1591/2009, legally represented by Mr. [REDACTED], as administrator.

Considering the following:

I. Premise

1. Intimation pursuant to Article 56 of GDPR

By the IMI application no. 159285 (registered at the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal under no. 21372 of the 28th of October 2020), pursuant to Article 56 of 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 – hereinafter “GDPR”), in order to identify the lead supervisory authority (LSA) and of the concerned supervisory authorities (CSA), the Polish Data Protection Authority (DPA) has informed all EU authorities that it has received a complaint against Cylex International Information Technology Societate în Nume Colectiv, enclosing evidence to that effect, in the English and Polish languages. DPA Poland considers the Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (hereinafter referred to as “ANSPDCP”) as the lead supervisory authority (LSA) in this case, given the fact that this company is based in Romania. DPA Poland also mentioned that the website is also available in Norwegian, French, Spanish, German, Slovak and Swedish. The proposal of the DPA Poland proposal was accepted by ANSPDCP.

2. Object and assessment of the complaints

Mrs. [REDACTED] lodged a complaint with the Polish authority on the 4th of August 2019 claiming that her personal data (name, surname, profession, address, a form of legal organisation which is no longer valid) are published, inter alia, on the website **cylex-polska.pl**. The petitioner addressed by e-mail invoking Articles 17 and 21 of the GDPR in order to obtain the deletion of these data that were published without her consent and information. The request was sent in Polish from the address [REDACTED] to the address info@cylex.pl on the 13th of June 2019.

It is noted that the **cylex site, owned by Cylex Tehnologia Informatiei Internațională Societate în Nume Colectiv** (hereinafter referred to as "Cylex"), through which are made public also the personal data of natural persons from different EU Member States, is available in various versions of European domain names and in the national languages of the EU Member States (such as: Romanian, French, Italian, Finnish, Spanish, German, Slovak, Swedish, Hungarian, Polish, Czech, Danish, Dutch), thus carrying out cross-border processing in the meaning of Article 4 point 23 of the GDPR. Considering that the Cylex headquarters is in Romania, ANSPDCP is the lead supervisory authority in this case, within the meaning of Articles 56, 60 and the following of the GDPR.

3. Investigation at Cylex Tehnologia Informatiei Internațională Societate în Nume Colectiv

Pursuant to Articles 57 and 58 of the GDPR and of Article 14 and the following from Law no. 102/2005 on the set up, organisation and functioning of the National Authority for the Supervision of Personal Data Processing, republished, it was ordered to carry out an investigation to handle the issues reported to the supervisory authority.

ANSPDCP sent the investigation letter to Cylex no. 1304 of the 22nd of January 2021, completed with the letter no. 5510 of the 26th of March 2021.

Cylex replied with the letter no. 22 of the 15th of February 2021, registered at ANSPDCP under no. 3051 of the 19th of February 2021, completed with the answer registered at ANSPDCP under no. 5534 of the 26th of March 2021.

Cylex's representatives stated the following:

- the identification elements of Mrs. [REDACTED] from the CYLEX catalogue were: the name of the professional, the address declared as headquarters of the professional, the KRS registration number in the Polish Trade Register of the professional, the NIP number meaning the fiscal attribute of the professional, issued by the Polish authorities, the field of activity (Laboratories – Services);
- Cylex collected these information from the public database of the Polish Trade Register (Statistic);
- Cylex does not object to the deletion of data either they come from companies or they belong to other categories of professionals;
- the deletion option is accessible from the profile of the professional, without the need to notify Cylex;
- by error, the request of Mrs. [REDACTED] was not processed properly, whereas the e-mail from the 13th of June 2019 went directly into spam; whereas the amount of spam e-mails is very large, the moderators have omitted to open and process the e-mail; usually, such requests are processed within 24 hours on weekdays or 72 hours on weekends and holidays;
- consequently, Cylex found out about the petitioner's request after receiving ANSPDCP's letter, i.e. on the 5th of February 2021; as such, Cylex deleted without delay all data belonging to the professional and submitted a request of deletion from Google cache; it has also taken measures to ensure that all e-mails are read and processed with the utmost rigor;
- Cylex informed the petitioner of the measures adopted by e-mail, on the 10th of February 2021.

Following the investigation carried out, pursuant to Article 60 (3) of the GDPR, ANSPDCP communicated electronically on the 7th of May 2021 a draft decision and the response sent by Cylex to the other personal data protection authorities in the European Union, the authorities in Berlin (and Bavaria) and Poland making relevant and reasoned objections on the 4th of June 2021.

By taking into account the objections thus formulated, in accordance with Article 60 (4) of the GDPR, ANSPDCP revised the draft decision, resulting in this decision.

4. Replies of other supervisory authorities in IMI

- A. In the notification based on Article 56 of IMI with no. 159285 (opened on the 27th of October 2020), in addition to the Polish authority, the following authorities were declared concerned authorities: Norway, Ireland, Germany - Lower Saxony, Belgium, Italy, Germany - Mecklenburg-Western Pomerania, France, Germany - Berlin, Slovakia, Sweden, Spain, Germany - Bavaria, Finland, as the processing would or could substantially affect the data subjects in their country.

Apart from the Polish authority, no other authority has stated that it has received any complaints against Cylex.

- B. Following the introduction of a first draft of the decision issued by ANSPDCP in IMI (Article 60 295321 - introduced on the 7th of May 2021), the authorities in Berlin (and Bavaria) as well as the Polish authority raised relevant and reasoned objections to IMI, with the proposal to ascertain the violation, mainly, of the provisions of Articles 6, 14, 12 (3), 17 (1), 24 of the GDPR.

The Italian authority also commented on the procedural issues (form of the draft decision).

C. Following the objections raised, ANSPDCP revised the draft decision and reintroduced it in IMI (Article 60 311339 - introduced on the 15th of July 2021), and the Berlin authority stated that it agrees with the proposed measures. As no other relevant and reasoned objections were raised, this final decision was issued.

5. The minutes of the finding

Following the investigation carried out and the consultations carried out with the other personal data protection authorities, the finding report no. 14199 of the 9th of August 2021 by which the following facts were ascertained was concluded:

1. "At the date of these minutes, it is noted that Cylex International Information Technology Societate în Nume Colectiv, with the headquarters mentioned on the first page of these minutes, did not handle the request of Ms. [REDACTED] of the 13th of June 2019, formulated based on Article 17 of the GDPR, respectively, did not send a reply within the deadlines provided by Article 12 (3) of the GDPR, the request being effectively resolved between the 5th and 10th of February 2021, according to the findings of these minutes. Pursuant to Article 24 of the GDPR, the controller is obliged to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing is performed in accordance" with the GDPR, including "appropriate data protection policies", which must include appropriate and effective measures to ensure that any request received at the address provided publicly as a contact to be assessed and handled under the conditions and deadlines provided by Articles 12-22 of the GDPR.

This deed constitutes the contravention provided by Article 12 of Law no. 190/2018, by reference to the provisions presented in Article 83 (5) letter b) of the GDPR.

2. At the date of these minutes, it is noted that Cylex Tehnologia Informației Internațional Societate în Nume Colectiv, with the headquarters mentioned on the first page of these minutes, has not presented evidence so far that it has provided complete information and in compliance with the provisions of Articles 12-14 of the GDPR to Mrs. [REDACTED], including information regarding the legal basis

of the processing provided by Article 6 of the GDPR, whose personal data were available on cylex-polska.pl until the period 5th – 10th of February 2021.

This deed constitutes the contravention provided by Article 12 of Law no. 190/2018, by reference to the provisions presented in Article 83 (5) letter b) of the GDPR."

Since in this case Cylex International Information Technology Societate în Nume Colectiv performs a cross-border processing, the provisions of Article 60 of Regulation (EU) 679/2016, as well as those of Article 16 (3), (5), (6), (7) of Law no. 102/2005, republished, which provide for the application of sanctions / corrective measures by decision of the president of ANSPDCP, which is based on the minutes of the finding and the report of the control staff, become applicable.

II. REASONS:

Having regard to the conclusions of the investigation carried out at Cylex International Information Technology Societate în Nume Colectiv,

Taking into account the relevant and reasoned objections raised by the other concerned supervisory authorities in IMI,

Based on the aspects retained and recorded in the minutes of finding no. 14199 of the 9th of August 2021, according to which:

1. "Cylex's representatives declared that they manage over 30 catalogues of online companies, with a database of over 60 millions companies (companies, institutions and other legal forms), having millions of clients all around the world"; "the CYLEX catalogue of companies is a search engine, in the sense that, specifically, the public records are accessed online and transferred to the CYLEX company catalog. In terms of features, the web catalog does not differ significantly from other search engines, such as Google, which also captures company pages and displays the related data in their link pages";
2. the purpose declared by the Cylex's representatives by processing these information is to offer "users a quick and easy way to find anywhere the products and services they are looking for, the purpose of the undersigned being to facilitate connections between companies and customers", so that entities can benefit from free registrations to promote their companies online and to gain customers";
3. Cylex's representatives also declared that "Cylex catalogs do not target data of individuals but strictly of professionals", the information being collected from public databases such as the trade registers from different countries;
4. in the case of professionals (as was the case with Mrs. [REDACTED]), the information collected and published in Cylex's online catalog also includes first and last name, address, other contact details, which allow the identification of a natural person and therefore constitute "personal data", in the meaning of the definition given by Article 4 point 1 of the GDPR ("any information concerning an identified or identifiable natural person ('data subject'); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifying element, such as a name, an identification number, location data, an online identifier, or one or more specific elements, specific to his physical, physiological, genetic, mental, economic, cultural or social identity");
5. consequently, all situations in which Cylex processes information that allows the identification of individuals, even if they are related to their professional activity, fall within the material scope of the GDPR, according to Article 2 (1);
6. as such, Cylex is obliged, as a personal data controller, to ensure the legality of the data processing of these persons, according to Articles 5 and 6 of the GDPR, to provide complete information, "in a concise, transparent, intelligible and easily accessible form, using a clear and simple language", according to Articles 12-14 of the GDPR, including information regarding the processing of data of these persons and, respectively, to respect the rights of these persons, as they are provided by Articles 15-22 of the GDPR, facilitating, at the same time, their exercise;

7. in this regard, it is necessary to duly supplement the existing information on each language version of the sites belonging to Cylex, on which online catalogues containing personal data of these persons are made available to the public;
8. according to Articles 13 and 14 of the GDPR, among the information that must be brought to the knowledge of the data subjects is also the legal basis of the processing, which must be established by reference to the provisions of Article 6 of the GDPR;
9. the legitimate interest (Article 6 (1) (f) of the GDPR) may constitute a valid legal basis in so far as the criteria set out in recital (47) of the GDPR are met: "The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. (...)";
10. in situations where, following the evaluation carried out by the controller, it is concluded that the legitimate interest does not meet these criteria, the only legal basis allowed for the data processing of the above mentioned persons is the consent of the data subjects (Article 6 (1) letter a) of the GDPR);
11. regarding the particular situation reported, of Ms. [REDACTED], although her request of the 13th of June 2019 reached the computer system of Cylex (in the spam folder), it was not handled within the legal deadlines provided by Article 17 (1) and Article 12 (3) of the GDPR (maximum one month or maximum 3 months), deleting her data and sending a reply taking place much later, after receiving the ANSPDCP letter no. 1304 of the 22nd of January 2021, respectively, during 05.02.2021-10.02.2021; from the 8th of February 2021, according to the statements of the Cylex's representatives, measures were taken so that "all e-mails are read and processed with maximum rigour";
12. therefore, until the 8th of February 2021, Cylex did not "implement" adequate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance" with the GDPR, including "appropriate data protection policies", as provided by Article 24 of the GDPR; thus, it is the obligation of the controller to implement appropriate and effective measures to ensure that any request received at the address provided publicly as a contact to be assessed and handled under the conditions and deadlines provided by Articles 12-22 of the GDPR;
13. or, in the case of Mrs. [REDACTED], her request made based on Article 17 of the GDPR was not handled by Cylex without delay, respectively, within the deadlines provided by Article 12 (3) of the GDPR;
14. also, although ANSPDCP requested this information through the letter no. 1304 of the 22nd of January 2021, Cylex did not present evidence regarding the provision of information to Mrs. [REDACTED] whose personal data were published on the website cylex-polska.pl, according to the provisions of Articles 12-14 of the GDPR and according to the above considerations in this context;
15. this conduct of the controller must be sanctioned, in order to avoid the recurrence of similar incidents in the future and to prevent the violation of the rights of other persons whose personal data they process. When imposing the sanction, it will be taken into account that, according to the records of ANSPDCP, no other similar complaints were received against Cylex regarding the exercise of rights under the GDPR, the above circumstances, the categories of data concerned and the fact that the controller took measures in order to remedy the notified issues",

Pursuant to Articles 14, 15 and 16 of Law no. 102/2005, republished, of Article 12 of Law no. 190/2018, in conjunction with Article 83 (2) and with the dispositions listed in Article 83 (5) letter b) of Regulation (EU) 679/2016, corroborated with the provisions of Article 58 (2) letters b) and d), as well as of Article 60 of Regulation (EU) 679/2016, related to the provisions of Articles 24, 25 and 26 of the Investigation Procedure, approved by the Decision of the President of ANSPDCP no. 161/2018,

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal

ORDERS

the following measures against Cylex Tehnologia Informației Internațional Societate în Nume Colectiv:

1. Issuing a reprimand for the deed ascertained through the minutes no. 14199 of the 9th of August 2021, based on Article 58 paragraph (2) letter b) of Regulation (EU) 2016/679, by reference to the infringement of Articles 17 and 12 (3) of this Regulation;
2. Issuing a reprimand for the second deed ascertained through the minutes no. 14199 of the 9th of August 2021, based on Article 58 paragraph (2) letter b) of Regulation (EU) 2016/679, by reference to the infringement of Articles 12-14 of this Regulation;
3. Imposing the corrective measure provided by Article 58 (2) letter d) of Regulation (EU) 2016/679 to implement appropriate technical and organisational measures in order to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR, including appropriate data protection policies, which shall include appropriate and effective measures so that any request received at the address provided publicly as a contact shall be assessed and handled under the conditions and deadlines provided by Articles 12-22 of the GDPR – deadline: 30 days from the date of communication of this decision;
4. Imposing the corrective measure provided by Article 58 (2) letter d) of Regulation (EU) 2016/679 to ensure the legality of the processing of data of natural persons whose personal data are available through online catalogues, according to Articles 5 and 6 of the GDPR and to provide complete information “in a concise, transparent, intelligible and easily accessible form, using a clear and simple language”, pursuant to Articles 12-14 of the GDPR, regarding the processing of data of these persons, respectively, to respect the rights of these persons, as they are provided by Articles 15-22 of the GDPR, facilitating, at the same time, their exercise; in this regard, it is necessary to properly supplement the existing information on each language version of the sites belonging to Cylex International Information Technology Societate în Nume Colectiv, on which online catalogues are made available to the public – deadline: 30 days from the date of communication of this decision.

Cylex Tehnologia Informației Internațional Societate în Nume Colectiv shall communicate to ANSPDCP the measures adopted for the implementation of the corrective measures within 45 days from the communication of this decision.

This decision was subject to the procedure provided for in Chapter VII of Regulation (EU) 2016/679, being sent for approval to all concerned supervisory authorities.

This decision, together with the minute no. 14199 of the 9th of August 2021 shall be communicated to **Cylex Tehnologia Informației Internațional Societate în Nume Colectiv** that has the right to challenge them pursuant to Article 17 of Law no. 102/2005:

“Article 17

(1) The data controller or processor may file an appeal against the report of the finding/sanctioning and/or the decision to apply the corrective measures, as the case may be, with the administrative

contentious section of the competent court, within 15 days from handing, respectively from communication. The decision resolving the appeal can be appealed only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.

(2) The report of finding/sanctioning or the decision of the president of the National Supervisory Authority unchallenged within 15 days from the date of handing, respectively the communication, constitutes an enforceable title without any other formality. Introducing the appeal provided in paragraph (1) suspends only the payment of the fine, until a final court decision is issued.

(3)The deadline of payment of the fine is 15 days from the date of handing, respectively from the date of communication of the minutes of finding/sanctioning or of the decision of the president of the National Supervisory Authority.”

President,



Summary Final Decision Art 60

Notification

No sanction

EDPBI:DEBE:OSS:D:2020:132

Background information

Date of final decision: 5 August 2020

Date of broadcast: 5 August 2020

LSA: DE-Berlin

CSAs: AT, BE, DK, FI, FR, DE, HU, IE, IT, LV, LT, NL, NO, PL, PT, SI, ES, SE, SK, UK

Controller: Applause GmbH

Legal Reference: Personal data breach (Articles 33 and 34)

Decision: No sanction

Key words: Personal data breach

Summary of the Decision

Origin of the case

Due to an employee's error, a document with personal data on people participating in a company project as testers was published on a digital platform. In addition, the responsible user made the entry publicly accessible on the web.

Findings

The controller deleted the document and the entry and reminded once against its employees that the use of this online platform is not permitted within the company. The controller informed also the data subjects in writing about the personal data breach.

Decision

In view of the measures the controller took to address the personal data breach or to mitigate its adverse effects, to prevent further risks, and its communication of the data breach to the data subjects concerned, the LSA closed the case without sanction.

Summary Final Decision Art 60

Notification of data breach

No sanction

EDPBI:DEBE:OSS:D:2020:133

Background information

Date of final decision:	5 August 2020
Date of broadcast:	5 August 2020
LSA:	DE-Berlin
CSAs:	ES, IT
Controller:	AWIN AG
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No sanction
Key words:	Personal data breach, Hacking, Credentials

Summary of the Decision

Origin of the case

An attacker used a stolen list of user names (email addresses and passwords) to try to gain access to the systems.

The attacker used a leased botnet to automatically send many thousands of requests to systems from about 100 different IP addresses. During this attack, the attacker could then match some of the stolen credentials with those on the systems.

The attack was logged in the systems, but did not generate any warnings or trigger any of the defence mechanisms. The efforts put by the attackers made detection considerably more difficult.

Findings

Following the attack, the passwords of the affected accounts have been reset. A check for changes to the affected accounts was performed and these were reset if necessary. Improved detection and prevention has been implemented and multi-factor authentication for platform user logins is under

development. The password reset of the affected accounts prevented further consequences, such as the redirection of payments.

Decision

In view of the measures the controller took to address the personal data breach or to mitigate its adverse effects, the measures it will adopt to prevent future risks, and its communication of the data breach to the data subjects concerned, the LSA closed the case without sanction.

Summary Final Decision Art 60

Complaint

Data subject rights compliance order to controller

EDPBI:CYSA:OSS:D:2020:131

Background information

Date of final decision:	27 July 2020
Date of broadcast:	28 July 2020
LSA:	CY
CSAs:	AT, DK, FR, IE, IT, NO, SE
Controller:	F1 Markets Limited
Legal Reference:	Right of access (Article 15)
Decision:	Data subject rights compliance order to controller
Key words:	Data subject rights, right of access

Summary of the Decision

Origin of the case

The complainant sent an email to the controller requesting the closure of his account and access to his data on the basis of article 15 of the GDPR. According to the complainant, the controller did not reply to the access request and the complainant lodged a complaint with the data protection authority.

Findings

The LSA found that the email sent by the complainant, with which he requested access to his data, was never received as it was quarantined by the email security service and categorized as spam due to the applied information security IT measures for emails received from outside the controller. The account manager who also received the email assumed that it had an informative character and was under processing, since the established procedure for an account closure is to be forwarded only the team responsible for this (i.e. Customer Support Team). Following the investigation, the controller complied with the access request and provided all information required by the data subject, before closing the account.

Decision

Since the controller eventually complied with the access request and affirmed that, it is working with the IT department in order to find a solution to avoid similar incidents in the future and that it plans on organising training session for the staff that interacts with the clients properly, the LSA decided not to take further actions regarding this matter.



535.1764
631.283
CR 160663
DD 160668
FD 189177

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Berlin, 24 March 2021

Final Decision

The Berlin DPA closes the case

1. Facts concerning the data breach

- **Controller:** Hotel Lützow
- **Incident:** Employee revealed the log-in data for booking.com
- **Date of occurrence:** 13 May 2020
- **Date of acknowledgement of the incident:** 13 May 2020
- **EU/EEA Member States concerned, with the number of data subjects concerned:**
 - Belgium: 23
 - Bulgaria: 6
 - Denmark: 40
 - Germany: 882
 - Estonia: 11
 - Finland: 25
 - France: 101
 - Greece: 25
 - UK: 192
 - Ireland: 20
 - Italy: 185
 - Croatia: 2
 - Latvia: 14
 - Lithuania: 12
 - Malta: 12
 - Netherlands: 81
 - Norway: 11
 - Austria: 31
 - Poland: 55
 - Portugal: 31
 - Romania: 19
 - Sweden: 26
 - Slovakia: 2
 - Slovenia: 20
 - Spain: 167
 - Czech Republic: 10
 - Hungary: 21
 - Cyprus: 1

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

Total: 2033

- **Category of data subjects:** Customers with bookings for the timespan between 15 May 2019 and 31 May 2021
- **Category of the data types/data records concerned:** First name, last name, telephone no., nationality, date of arrival and departure, partially credit card no. (without security number)
- **Likely consequences of the violation of the protection of personal data:**

2. Description of the data breach from a technical-organizational perspective

An attacker was given access to the booking.com account of the controller person for about 4 hours. The access data was obtained by a call from the attacker to an employee of the controller, whereby the attacker pretended to be an employee of booking.com. The employee provided the access data by telephone.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

- Blocking of the account by boooking.com within 4 hours after the access data has been obtained.
- Changing the access data
- Training of the controller's employees by booking.com.
- Data protection audit by the company's data protection officer

The Berlin DPA considers the measures taken to be sufficient.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The data subjects concerned were notified in writing, some of them initially by e-mail. Finally, the controller published a data protection notice on his homepage (German, English, Italian).

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

Booking.com has a system that attempts to detect potentially problematic account accesses. This system has also resulted in the prompt verification and blocking of the account.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

See 3.

7. Taken measures by the LSA Berlin DPA

7.1 Taken measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA proposes to close the case.

7.2 Taken measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has also not identified any data protection violations beyond Articles 33, 34 GDPR.

Your reference nr: 306693

Diarienummer:
DI-2021-8549**Datum:**
2025-01-08

Decision

You have sent a report that was received by the Swedish Authority for Privacy Protection (IMY).

IMY is currently not taking any action as a result of your report.

Please note that in the event of a future complaint or supervisory case, IMY may take the report in consideration.

The case is closed.

**Postadress:**
Box 8114
104 20 Stockholm**Webbplats:**
www.imy.se**E-post:**
imy@imy.se**Telefon:**
08-657 61 00

COMPLAINANT

See appendix

CONTROLLER

SkatePro ApS

Swedish ref.:
IMY-2023-113**IMI ref.:**
IMI A56 534978**IMI case register:**
563146**Date:**
2025-02-19

Decision under the General Data Protection Regulation

Decision of the Authority for Privacy Protection

IMY adopts the Danish Data Protection Authority's decision in Appendix 1 pursuant to Article 60(8) of the General Data Protection Regulation (GDPR) and closes the case.

Presentation of the supervisory case

On the 4th of January 2023 the complainant filed his complaint with the Swedish Authority for Privacy Protection (IMY). On the 5th of July 2023 IMY sent the complaint to the Danish Data Protection Authority as the case concerns cross-border processing and SkatePro ApS has its main establishment in the Netherlands. The Danish Data Protection Authority has investigated the matter and issued a decision pursuant to Article 60(3) GDPR. None of the supervisory authorities concerned has expressed an objection to the draft decision pursuant to Article 60 (4) GDPR.

Statement of reasons for the decision

The Danish Data Protection Authority has stated in its draft decision that the investigation has shown that SkatePro has now deleted the complainants personal information from all their systems, and that SkatePro does not seem to use "forced consent" as addressed in your complaint, as present.. In light thereof and that none of the supervisory authorities concerned have expressed an objection to the draft decision IMY adopts the decision pursuant to Article 60(8) GDPR.

The case is therefore closed.

Postal address:
Box 8114
104 20 Stockholm
Sweden**Website:**
www.imy.se**E-mail:**
imy@imy.se**Telephone:**
+46 (8) 657 61 00**Appendix**

The complainant's personal data

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

DRAFT

COMPLAINANT**CONTROLLER**
Morrow Bank ASA**Swedish ref.:**
DI-2022-558**Norwegian ref.:**
23/01372-5**IMI case register:**
544525**Date:**
2025-02-14

Final decision under the General Data Protection Regulation – Morrow Bank ASA

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection's (hereinafter "IMY") adopts the following decision on the complaint submitted against Morrow Bank ASA on 23 January 2022 (Case DI-2022-558):

- The complaint shall be rejected pursuant to Article 60(8) of the General Data Protection Regulation (GDPR)¹.

Factual Background

On 7 January 2022, Morrow Bank sent an email to the data subject residing in Sweden (hereinafter the "complainant") informing that it would update its privacy policy to include a section about disclosure of contact information to third parties, such as Facebook and Google for customer matching purposes. This matching would entail that those customers would be shown relevant information and marketing on social media, search engines and websites.

In the updated privacy policy, Morrow Bank stated that it would rely on Article 6(1)(f) of the GDPR as the lawful basis for this disclosure for customer matching purposes.

Customers were informed that they had a right to object to this specific disclosure by signing into the portal at the bank's website. Thus, the disclosure would happen by default unless customers explicitly opted-out by objecting.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

Morrow Bank and its partners by email and SMS at the time of becoming a customer in July 2020, he wrote an email to Morrow Bank on 9 January 2022, inquiring why the bank had decided to disclose his email and phone number to these third-party partners without his consent. On 18 January 2022, the complainant sent a follow-up email where he informed Morrow Bank that he would lodge a complaint to IMY unless the

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).

bank made changes as to how the contact information is disclosed to third parties. The emails to dpo@komplettbank.no remained unanswered.

According to the complainant, it could not reasonably be expected that a licensed bank would disclose its customers' contact information to third parties such as Facebook and Google for the purpose of consumer matching, at the time of becoming a customer in July 2020. As such, the complainant holds that the disclosure of contact information under the "legitimate interests" clause in this specific case is unlawful.

Legal Background

The GDPR lays down the provisions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

'personal data' means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Pursuant to Article 4(2) GDPR:

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Article 77(1) GDPR states that:

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

Findings

In the context of the investigation regarding the present case, Morrow Bank states that they never processed customer's personal data for consumer matching purposes.² Indeed, it changed its privacy policy in 2022 as preparation, in case it would be relevant. However, such processing never started.

Furthermore, Morrow Bank has now changed its privacy policy and removed the information on customer matching.³

In light of the above, it appears that Morrow Bank never processed the personal data (within the meaning of Article 4(1) and (2)) of the complainant for customer matching

² See Morrow Bank's reply to Datatilsynet's order to provide information, dated 6 December 2024.

³ Ibid.

purposes. It follows directly from the wording in Article 77(1) that the data subject must bring forward that their personal data has been processed in a way that infringes the Regulation.

Consequently, the complainant's submission to IMY does not constitute a complaint within the meaning of Article 77 GDPR.

Having considered the above, the complaint shall be rejected in accordance with Article 60(8) GDPR.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision

This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision. Only the Swedish version of the decision is deemed authentic

Diarienummer:
DI-2022-558

The complainant
Morrow Bank ASA

Datum:
2025-02-06

Decision under the General Data Protection Regulation

Decision of the Authority for Privacy Protection

IMY adopts the Norwegian Data Protection Authority's decision in Appendix 1 pursuant to Article 60(8) of the General Data Protection Regulation (GDPR) and closes the case.

Presentation of the case

On January 23, 2022 the complainant filed his complaint with the Swedish Authority for Privacy Protection (IMY) against Komplett Bank ASA (Morrow Bank ASA). On March, 30 2023 IMY sent the complaint to the Norwegian Data Protection Authority as the case concerns cross-border processing and Morrow Bank ASA has its main establishment in the Netherlands. The Norwegian Data Protection Authority has investigated the matter and issued a decision pursuant to Article 60 (3) GDPR. None of the supervisory authorities concerned has expressed an objection to the draft decision pursuant to Article 60 (4) GDPR.

Statement of reasons for the decision

The Norwegian Data Protection Authority has stated in its draft decision that the investigation does not show that the case concerns processing of personal data, since the planned processing that the complaint concerns never occurred, and that the letter from the complainant therefore does not constitute a complaint according to Article 77 in the GDPR. Nor IMY or any other concerned authority has expressed any opinions on the decision. In light thereof IMY adopts the decision pursuant to Article 60(8) GDPR.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

The case is therefore closed.

Maja Welander

Appendices

1. *The Norwegian Data Protection Authority's draft decision*
2. *The complainants personal data*

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision

Reference
number:
IMY 2024 2011

Date:
2025-02-21

Decisions under the General Data Protection Regulation

Decision of the Privacy Protection Authority

Case closed.

Presentation of the case

On 17 March 2024, you submitted a complaint to the Swedish Data Protection Authority (IMY). Your complaint shows that Norwegian Air shared your and leaked your personaldata. IMY has submitted your complaint to the Norwegian Supervisory Authority (Datatilsynet) as lead supervisory authority pursuant to Article 56 of the Data Protection Regulation¹. In accordance with Article 60(3), the DPA has submitted a draft decision (seeAnnex) to the other supervisory authorities concerned. None of the supervisoryauthorities concerned has objected to the draft.

Reasons for the decision

Pursuant to Article 57(1)(f) of the GDPR, supervisory authorities are to process complaints from a data subject and, where appropriate, investigate the subject matter of the complaint. On behalf of the Swedish Data Protection Authority, IMY has given you the opportunity to complete the case on two occasions on 22 October and 2 December 2024. You have not submitted any additional documents.

The Swedish Data Protection Authority's draft decision states, inter alia, the following. In view of the fact that the complainant has not submitted any evidence in support of its complaint, the Swedish Data Protection Authority considers that there are no grounds for further investigation of the complaint. Since none of the supervisory authorities concerned has objected tothe DPA's draft decision, the draft decision is binding under Article 60(6) of the GDPR. Against this background, IMY is to adopt a decision closing the case.

The case should therefore be closed.

1(2)

Postal address:

Box 8114
104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Telephone:

08-657 61 00

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).

Annex:

The Swedish Data Protection Authority's draft decision translated into Swedish

How to appeal

If you want to appeal the decision, you should write to the Privacy Protection Authority. Please indicate in your letter the decision you are appealing against and the amendment you are requesting. The appeal must have been received by the Integrity Protection Authority no later than three weeks from the day you received the decision. If the appeal has been received in due time, the Integrity Protection Authority will forward it to the Administrative Court in Stockholm for consideration.

N may email the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The contact details of the authority can be found on the first page of the decision

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

COMPLAINANT

See appendix

CONTROLLER

Klarna Bank AB

Diarienummer:
IMY-2022-10270

Case number at the German supervisory authority
521.16090

IMI case register:
334404

Datum:
2025-03-25

Decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Klarna Bank AB (556737-0431) has processed personal data in breach of Article 15 and Article 12(3) of the General Data Protection Regulation (GDPR)¹ by not providing the complainant with access to his personal data and other supplementary information without undue delay following a request made by the complainant.

IMY issues a reprimand to Klarna Bank AB pursuant to Article 58(2)(b) of the GDPR for the infringement found.

Presentation of the supervisory case

IMY has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint regarding the right to access. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complaint has been lodged (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Austria, Denmark, Finland, France, Germany, Italy and Norway.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

The complainant states, in essence, as follows. The complainant has requested access to his personal data from Klarna on 19 January 2022 but has not received a reply to his request.

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).

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

Klarna has essentially stated the following. Klarna is the data controller for the processing that is the subject of the complaint. The company has received a report of fraud from the complainant in which a request for access was also expressed. It has not been possible to verify the date of receipt of the notification, but an internal case has been created on 15 April 2022. Klarna's customer service, which specialises in fraud, has handled the notification in accordance with the fraud case procedure and notified the complainant on 5 September 2022. On the basis of the documentation, it appears that the customer service employee did not understand the complainant's request for access, but only handled the fraud case. Perceiving requests under the General Data Protection Regulation is something that all customer service employees have been trained in, that it does not seem to have been done in this case has been due to an individual mistake by the customer service employee. Klarna has contacted the complainant on 21 November 2024 and announced that it intends to comply with the request. Klarna has asked for a telephone number in order to be able to send a verification code to open the register extract and intends to send the extract as soon as the complainant has submitted it.

IMY submitted Klarna's statement to the supervisory authority in Germany in order to give the complainant the opportunity to comment on it, but no reply was received by IMY.

Reasons for the decision

Controller

According to Article 4(7) of the GDPR, 'controller' means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Klarna has stated that the company is the controller for the personal data processing to which the complaint relates, which is supported by the investigation in the case. IMY therefore considers that Klarna in question is the data controller for the processing covered by the supervision.

Klarna's handling of the complainant's request for access

It follows from Article 15 of the GDPR that the controller is obliged to inform any person who so requests whether or not personal data relating to the applicant are being processed. If such data are processed, the controller shall, in accordance with Article 15 of the GDPR, provide the data subject with additional information concerning, inter alia, the purposes of the processing and the recipients of the data, as well as a copy of the personal data processed by the controller. It follows from Article 15(1) and (2) what additional information is to be provided to the data subject. Article 15(3) requires the controller to provide the data subject with a copy of the personal data undergoing processing.

Pursuant to Article 12(3) of the GDPR, upon request, the controller shall provide the data subject, without undue delay and in any event no later than one month after receiving the request, with information on the measures taken pursuant to Article 15 of the GDPR. That period may be extended, if necessary, by a further two months, taking into account the complexity of the request and the number of requests received. The controller shall notify the data subject of such an extension within one month of receipt of the request, stating the reasons for the delay.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

The investigation into the case shows the following. Klarna has received the complainant's request for access. According to Klarna, it has not been possible to verify exactly when it received the complainant's request, but that a case related to the letter of 15 April 2022 has been created. On 26 November 2024, Klarna announced that it intended to comply with the request and that Klarna had contacted the applicant in that regard. Klarna also stated to IMY that the reason why the applicant's request had not been satisfied in the past was that an individual customer service employee had not taken note of the applicant's request for access.

IMY considers that, on the basis of the documentation, it may in any case be considered clear that Klarna received the complainant's request for access on 15 April 2022. After IMY commenced supervision of the company, Klarna contacted the applicant regarding its request for access. By that time, more than two and a half years had passed since Klarna had received the applicant's request. There is no indication that Klarna would have dealt with the complainant's request if IMY had not initiated supervision of the case. In the light of the above, IMY considers that Klarna acted in breach of Article 15 and Article 12(3) of the GDPR by not providing the complainant with access to his or her personal data and other supplementary information without undue delay.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case need to be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

With regard to the choice of intervention, IMY takes account of the following factors. Klarna has infringed Article 15 and 12(3) of the GDPR. The time which has elapsed since the request for access was made is relatively long. The infringement concerned a data subject; Klarna has pointed out that there has been a mistake in the individual case and that all customer service employees receive training in paying attention to requests under the General Data Protection Regulation. Klarna has now also contacted the applicant and that it intends to comply with the applicant's request. On an overall assessment, IMY considers that it is a minor infringement as referred to in recital 148 of the GDPR and that Klarna should therefore be given a reprimand for the infringement found.

This decision has been taken by Head of Unit Nidia Nordenström after presentation by legal advisor [REDACTED].

Notice: This document is an unofficial translation
of the Swedish Authority for Privacy Protection's
decision.

Appendix

The complainant's personal data

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

SA Ireland

Reference number:
IMY-2022-6649

Date:
2025-03-18

Decision on complaint

Decision of the Privacy Protection Authority

Case closed.

Reasons for the decision

The Swedish Data Protection Authority (IMY) has received a complaint from you against the company Resetera/M.O.B.A Network AB. The complaint shows that the company has not complied with your request for access to personal data (Article 15 of the GDPR).

The complaint has been transmitted to us by the supervisory authority of the country where you lodged your complaint (Ireland) in accordance with the provisions of the GDPR on cooperation in cross-border processing. IMY has handled the complaint as lead supervisory authority under Article 56 GDPR.

IMY shall process complaints about incorrect processing of personal data and, where appropriate, investigate the subject matter of the complaint (Article 57(1)(f) GDPR).

On 28 August 2024, IMY asked the IE SA to forward a letter to you. The Irish Data Protection Authority informed IMY on 4 September that the letter had been sent. The letter asked whether your complaint was still relevant. You were informed that a failure to reply within the two-week time limit would be interpreted as meaning that you wish to withdraw your complaint against Resetera/M.O.B.A Network AB, with the result that IMY would close the case.

On 11 September 2024, you replied in an email to the IE SA that, in view of the long time that has elapsed without anything happening, you were unsure whether there were grounds to keep the case active. For the avoidance of doubt, on 12 September the IE SA sent you a request for clarification as to whether you wish IMY to continue investigating your complaint. You have not subsequently provided any further reply to the Irish Data Protection Authority. Since no further reply has been received from you since then, IMY understands that you are no longer interested in pursuing the complaint.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se
Telephone:
08-657 61 00

Against this background, IMY decides not to investigate the complaint further.

Case closed.

How to appeal

If you want to appeal the decision, you should write to IMY. In your letter, please indicate the decision you are appealing against and the change you are requesting. The appeal must be received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in due time, IMY will forward it to the Administrative Court in Stockholm for consideration.

You can email the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The contact details of the authority can be found on the first page of the decision.

COMPLAINANT

See annex

CONTROLLER

Klarna Bank AB

Swedish reference number:
DI-2022-1665**Austrian reference number:**
D130.763**IMI case register:**
334404**Date:**
2025-03-10

Final decision pursuant to Article 60 under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Data Protection Authority finds that Klarna Bank AB (organisation registration number 556737-0431) has failed in its responsibilities under

- Article 12(2) of the GDPR¹ by, when the complainant submitted a request of access under Article 15 of the GDPR to Klarna Bank AB:s customer service (in Sweden and then Germany) on August 14th 2021, directing the complainant to submit a new data subject rights request to the customer service of the correct country (Austria).
- Article 12(3) of the GDPR by not complying with the complainant's data subject rights request dated August 14th 2021 until February 16th 2022.

Klarna Bank AB has therefore neither facilitated the complainant's exercise of their right of access under Article 15 of the GDPR in accordance with Article 12(2) of the GDPR in connection with the complainant's request of August 14th 2021, nor satisfied the complainant's right of access without undue delay in accordance with Article 12(3) of the GDPR.

The Swedish Authority for Privacy Protection notes on the other hand that it is not apparent from the investigation in the case that Klarna Bank AB has failed to comply with Article 15 of the GDPR in the way alleged in the complaint.

The Swedish Data Protection Authority issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringements of the Articles 12(2) and 12(3) of the GDPR.

Postal address:
Box 8114
104 20 Stockholm
Sweden**Website:**
www.imy.se**E-mail:**
imy@imy.se**Telephone:**
+46 (8) 657 61 00

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).

Presentation of the supervisory case

The handling of the case

The Swedish Data Protection Authority (IMY) has initiated a supervision against Klarna Bank AB (Klarna) due to a complaint. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complaint has been lodged (Datenschutzbehörde, Austria) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Austria, Norway, Germany, France, Italy, Denmark and Finland.

In response to the complaint, IMY has initiated a supervision in order to investigate whether Klarna has facilitated the exercise of the complainant's right of access under Article 15 of the GDPR in accordance with Article 12(2) of the GDPR without undue delay in accordance with Article 12(3) of the GDPR. Furthermore, IMY has initiated the supervision in order to investigate whether the complainant's requests for information and access have been properly received and handled (Article 13(1)(c) and Article 15 of the GDPR).

In view of the fact that a further investigation in the matter of Article 13(1)(c) would not be appropriate under Article 57(1)(f) of the GDPR, IMY has decided to only further investigate the complaint in the matter of the Articles 12 and 15 of the GDPR.

The complaint

The complainant has essentially stated the following. The complainant has submitted a request of access under Article 15 of the GDPR to Klarna on August 14th 2021. The reply that he has received from Klarna on August 25th 2021 did not contain the information he had requested, but only information about Klarna's general principles of data protection on the internet. Therefore Klarna has not facilitated his exercise of his right of access under Article 15 of the GDPR.

What Klarna has stated

Klarna is the data controller for the processing in question and has essentially stated the following.

Measures taken by Klarna

On August 14th 2021, the complainant, a customer of Klarna in Austria, submitted a request of access under Article 15 of the GDPR, which was received by Klarna's Swedish customer service. Due to the fact that the complainant's request was written in German, the case has been transferred to Klarna's German customer service department (the German General Customer Service).

On August 25th 2021, one of Klarna's case handlers at the German General Customer Service has sent a reply to the complainant's request by email. In this reply, the responsible case handler has, inter alia, attached a link to a page with general data

protection information at Klarna's German customer service department for data protection (the German Data Protection Department).

It is likely that the Klarna case handler has directed the complainant to the German Data Protection Department due to an oversight when the case handler found that the complainant's request was written in German. When the error was discovered, another case handler from the General German Customer Service has sent a new reply to the complainant on the following day, August 26th 2021. In this new reply from the German General Customer Service, the relevant contact details to Klarna's Austrian data protection customer service department (the Austrian Data Protection Department) has been attached.

What Klarna has stated regarding compliance with Article 12 and 15 in the present case

On the basis of the provisions of Article 12(2) of the GDPR, it has not been clear at the time of the complaint what it means in more detail that the controller must facilitate the exercise of the data subject's rights. Nor has there been any EU-guidelines or guidance decisions in this area at the time. The information that has been available at the time has however been guidelines issued by the Irish Data Protection Authority in 2019 stating that a controller may invite or redirect a data subject who has made a data subject rights request (DSR request(s)), made pursuant to Articles 15–22 GDPR, to send it via a dedicated form instead.²

On August 26th 2021, the German General Customer Service case handler has facilitated exercising the complainant's DSR request by providing clear information to him on the procedure to be followed. The case handler has also provided him contact details to the Austrian Data Protection Department in order to ensure that his DSR request would be handled in the best and most efficient way and in accordance with best practice in Austria. Klarna has been accommodating by handling the complainant's DSR request in August 2021. Klarna's conduct at the time has therefore been compliant with Article 12(2) and (3) of the GDPR.

In addition, despite previous handling, Klarna sent a copy of the complainant's personal data undergoing processing to the complainant on February 16th 2022.

What Klarna has stated regarding their work to safeguard the data subject's rights in compliance with Article 12

Since the case in question was handled at Klarna, the European Data Protection Board (EDPB) has, inter alia, developed guidelines on how a DSR request should be handled by a controller. Although the guidelines had not been published at the time of the complaint, Klarna has — both before the case in question and continuously afterwards — improved, simplified and streamlined their processes to ensure the data subjects' rights under the GDPR. Of relevance to the case at hand is that according to the new routines at Klarna today, it does not matter which customer service a DSR request is sent to, meaning to which country's customer service a customer turns. Klarna will today forward such a request internally to the right country's customer service instead of redirecting the customer to contact that customer service him- or herself.

² An Coimisiún um Chosaint Sonrai – Data Protection Commission. *Data Subject Access Requests – FAQs*. (2019). https://www.dataprotection.ie/sites/default/files/uploads/2019-10/FAQ%20Guide%20to%20Data%20Subject%20Access%20Requests_Oct19.pdf (Downloaded 2024-10-17)

Opinion of the complainant

On January 24th 2024 the complainant has been heard on Klarna's statement. The complainant has on January 31st 2024 essentially stated the following. It is possible that Klarna has processed his request. In any event, he has not received an answer in the sense of information at any time. He has not been under any obligation to contact the correct customer service office once he has turned to Klarna. Klarna has therefore not acted in accordance with Article 12(2) of the GDPR in that regard, since Klarna should have forwarded his request to the correct customer service.

It is not true that he received a copy of his personal data undergoing processing by Klarna on February 16th 2022.

Opinion of Klarna

On November 15th 2024 Klarna was heard on the complainant's opinion. On November 19th 2024 Klarna has stated the following. Klarna has sent the complainant a copy of his personal data undergoing processing by Klarna on February 16th 2022. In support of Klarna's statement on that point, Klarna has adduced the email correspondence that Klarna had with the complainant from February 16th 2022.

Opinion of the complainant

IMY sent the submissions of Klarna from November 19th 2024 to the Austrian Data Protection Authority Datenschutzbehörde on January 17th 2025 asking to communicate them to the complainant, to grant the right to be heard, with a time frame on 14 days and then come back to IMY, preferably no later than February 14th 2025. The Austrian Data Protection Authority did not revert to this.

Motivation for the decision

Applicable provisions

The controller shall facilitate the exercise of the data subject's rights under the Articles 15 to 22 of the GDPR. (Article 12(2) of the GDPR)

The controller shall provide information on action taken on a request under the Articles 15 to 22 of the GDPR to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. (Article 12(3) of the GDPR)

It further follows from Article 15 of the GDPR that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain specified information (right of access). (Article 15 of the GDPR)

It further follows from Article 57(1)(f) of the GDPR that IMY must process complaints from data subjects who consider that their personal data are being processed in breach of the GDPR. IMY is to examine, where appropriate, the subject matter of the

complaint. The Court of Justice of the European Union has stated that the supervisory authority must investigate such complaints with due diligence.³

Under 23 § of the Administrative Procedure Act⁴, an authority must ensure that a case is investigated to the extent required by its nature.

Assessment

The case

The investigation has shown that, at the time of the complaint, it was up to the data subject to resend a request for rights under Article 15 of the GDPR to the Klarna customer service of the country in which the data subject was resident, if the request was made to another country's customer service.

Legal provisions

Article 12(2) of the GDPR: facilitation of the exercise of data subject rights

It is true that, at the time of the complaint, there were no indicative clarifications provided by the EDPB clarifying what it means for the controller to facilitate the exercise of data subject rights. From the guidelines issued by the Irish Data Protection Authority in 2019 it has been said that in case of a received DSR request, it has been sanctioned that a controller or a processor invites or redirects a data subject to a more appropriate communication channel for the controller or the processor. Today, the legal position is clearer. Where a data subject makes a DSR request using a communication channel provided by the controller, the request of the data subject shall be handled, even if the controller prefers another channel.⁵

The meaning of the obligation to facilitate the exercise of, *inter alia*, a data subject's right of access under Article 15 of the GDPR has however already been elaborated in recital 59 of the GDPR at the time of the complaint. Recital 59 of the GDPR states that the controller should establish procedures to facilitate the exercise of data subject rights, including mechanisms for requesting and, where appropriate, accessing personal data free of charge.

For example, a controller is not considered having facilitated the exercise of the rights of a data subject in accordance with Article 12(2) of the GDPR where a data subject needs to delete his or her user account and create a new one in order to exercise the DSR in question.⁶ It is therefore the responsibility of the controller to facilitate the exercise of the data subject's rights by not requiring time-consuming further action from the data subject, like demanding the data subject to make a new DSR request to another e-mail address.

Furthermore, it is IMY's opinion that the EDPB Guidelines 01/2022 show broad support for interpreting, on the basis of Article 12(2) and recital 59 of the GDPR, that facilitation should not mean to require additional measures like those in this case. Klarna's argumentation that the EDPB Guidelines on access were not published at the time of the present case does not call that finding from IMY into question. IMY does not claim

³ Judgment in Schrems II, Case C-311/18, EU:C:2020:559, paragraph 109.

⁴ The Swedish Administrative Procedure Act (2017:900)

⁵ Stockholm Administrative Court of Appeal judgment of 7 June 2024 in case No 2639-23 and European Data Protection Board, (EDPB or European Data Protection Board (2023) *Guidelines 01/2022 on data subject rights – Right of access* (EDPB Guidelines 01/2022), p. 52 et seq.

⁶ Judgment of the Stockholm Administrative Court of Appeal of 7 June 2024 in case number 2639-23

that Klarna has been obliged to follow guidelines that were not available at the time of the complaint.⁷

Although there has not been any guidelines on Article 12(2) of the GDPR at the time of the complaint, there has still been an obligation for a controller to ensure that internal processes and systems have been in compliance with the provisions of the GDPR.⁸ By requesting the complainant to make a new DSR request to another recipient, Klarna has not facilitated the complainant's exercise of its right of access under Article 15 of the GDPR. In conclusion, IMY therefore finds that the requirements to facilitate the exercise of the data subject rights according to Article 12(2) of the GDPR has not been met at the time of the handling of the case by Klarna. Overall, therefore, IMY therefore concludes that Klarna has failed to fulfil its obligations under Article 12(2) of the GDPR.

Article 12(3) of the GDPR: time period for the provision of information

Based on what Klarna has stated in the case, the complainant's request has been handled on August 26th 2021, which the complainant has not objected to. The investigation has however shown that the complainant's request for access was not satisfied until February 16th 2022, which is more than one month after the request was received. It does not appear like the request has been of a particularly complex nature. Neither does it appear like Klarna has informed the complainant of the delay with a justification of an extended response time of two months in total in accordance with Article 12(3) of the GDPR. IMY therefore concludes that Klarna has failed to fulfil its obligations under Article 12(3) of the GDPR by not satisfying the complainant's request until February 16th 2022.

Article 15 of the GDPR: right of access

The complainant has disagreed that his request for access has been satisfied. IMY has asked Klarna to submit written evidence that the complainant's request for access has been satisfied. Klarna has by their submissions showed that the complainant's request for access has been satisfied, but not until February 22nd 2022. The complainant was then given the opportunity to comment on Klarna's statement.

IMY has not received any information from the complainant that contradicts these facts and finds no other reason to question the submissions from Klarna. IMY has therefore investigated the case to the extent required by Article 57(1)(f) of the GDPR and 23 § of the Administrative Procedure Act and notes that it is not apparent from the investigation that Klarna has failed to comply with Article 15 of the GDPR in the way alleged in the complaint.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83 of the GDPR. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2) of the GDPR, such as injunctions and prohibitions. Furthermore, Article 83(2) of the GDPR determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148 of the GDPR, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b) of the GDPR. Aggravating and mitigating circumstances of the case need to

⁷ See Stockholm Administrative Court's judgment of 22 December 2022 in case number 11453-22

⁸ Judgment of the Stockholm Administrative Court of Appeal of 7 June 2024 in case number 2639-23

be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY has considered the following relevant facts. The current supervision covers Klarna's handling of an individual complainant's request for access. In that regard, IMY found that Klarna failed to fulfil its responsibilities under Article 12(2) of the GDPR by failing to facilitate the complainant's request for access under Article 15 of the GDPR and its responsibilities under Article 12(3) of the GDPR by failing to deal with the complainant's request without undue delay.

Mitigating the infringement under Article 12(2) of the GDPR, it should be taken into account that Klarna has taken measures to facilitate the exercise of data subject rights under the GDPR through changes in their procedures. Some measures have already been taken before the opening of this supervisory case. As Klarna's procedures stand today, Klarna internally ensures that a received DSR request is sent to the right country's customer service, regardless of which customer service the request was sent to from the beginning, without the complainant having to make any new request. Furthermore, the identified infringement under Article 12(2) of the GDPR has occurred relatively far back in time (2021).

The current supervision also covers Klarna's handling of an individual complainant's request for access in the light of the requirements set out in Article 12(3) of the GDPR. In this regard, IMY has found that Klarna has failed to fulfil its obligations to satisfy the complainant's request in a timely manner. Although the prescribed time limit of a maximum of one month has been exceeded by more than six months, the fact that the complainant's right of access has been complied with may be considered in relation to the infringement under Article 12(3) of the GDPR. The infringement in question is therefore of a less serious nature than if the request had been left unanswered.

Against this background, IMY considers this a minor infringement within the meaning of recital 148 of the GDPR and that Klarna is to be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

Annex

The complainant's personal data

CONTROLLER
Spares Nordic AB

Swedish ref.:
IMY-2024-13575

Nat.ref no:
TSV/8789/2024

IMI case register:
602032

Date of the decision:
2025-03-06

Final decision under the General Data Protection Regulation – Spares Nordic AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) notes that Spares Nordic AB (556998-9444) has now complied with the applicant's request for access. In the light of the above, IMY finds no reason to take any further action in this case.

The case is closed.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision against Spares Nordic AB due to a complaint. The complainant has been submitted to IMY, as the lead supervisory authority under Article 56 GDPR, by the supervisory authority of the country (Finland) in which the complainant lodged its complaint in accordance with the Regulation's provisions on cooperation in cross-border processing.

Since it is a cross-border complaint, IMY has made use of the mechanisms got cooperation and consistency of the GDPR.

The complainant essentially states the following: The complainant requested access from Spares Nordic AB by email in accordance of article 15 GDPR on the 26th of July 2024.

Spares Nordic AB essentially states the following. Spares Nordic AB is the data controller in the matter. The company received the complainants request with questions on the 8th of June 2024. The company replied to the complainant on the 10th of June 2024 and referred to the page for personal data on the companys website. With this, the complainant received answers to all of his questions. However, the company notes that the customer has not been given access to his personal data. This was because the case handler who received the request was unsure how the case should be handled because the complainant was registered as a company (OY) and not as a private person. The companys IT department contacted the complainant to confirm his identity and sent all his personal data to him on the 4th of December 2024.

IMY has sent Spares Nordic AB statement to the supervisory authority of the country in which the complainant lodged its complaint to give the complainant opportunity to comment on Spares Nordic AB statement. The complainant has not responded.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

Reasons for the decision

The complainant has requested access. The right of access follows from Article 15 of the GDPR. The provision means that a data subject has the right to contact the controller and obtain confirmation as to whether or not personal data concerning him or her are being processed and, if so, have access to the personal data and certain information.

Spares Nordic AB has informed IMY that the company has now complied with the complainant's request for access. IMY finds no reason to question that this has happened. IMY notes that Spares Nordic AB has therefore now complied with the complainant's right to access. Against this background, IMY does not find any further action to be taken in this case.

The case should therefore be closed.

Appendix to decision

Complainants personal data

COMPLAINANT

See Annex

SYNSOBJEKT

TF Bank AB

Reference number:

IMY-2023-16160

Date:

[2024-12-19]

Final decision under the General Data Protection Regulation – TF Bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) notes that TF Bank AB, 556158-1041, in its handling of the complainant's request for access made on 2 September 2019, has processed personal data in breach of Article 12(3) of the GDPR¹ by failing to comply without undue delay with the complainant's right of access under Article 15 of the GDPR and by failing to inform the complainant without undue delay of the measures they have taken in response to the complainant's request for erasure under Article 17 of the GDPR.

The Swedish Authority for Privacy Protection issues a reprimand to TF Bank AB pursuant to Article 58(2)(b) GDPR for infringement of Article 12(3) GDPR.

Presentation of the supervisory case

Postal address:

Box 8114
104 20 Stockholm
Website:

www.imy.se

Due to the cross-border nature of the case, IMY has made use of the cooperation and consistency mechanisms found in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities of Finland and Germany.

E-mail:

imy@imy.se

Telephone:
08-657 61 00

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).

The complaint

IMY has initiated supervision of TF Bank AB in order to investigate a complaint about the right of access and the right to erasure.

The applicant states, in essence, as follows. The complainant responded to a marketing campaign and applied for a credit card from TF Bank AB. The bank did not accept the application without a signed original application form, and the complainant chose to withdraw the application. At the same time, on 2 September 2019, the complainant requested access to the personal data processed by the Bank concerning him pursuant to Article 15 of the GDPR. The complainant also requested that his data be deleted in accordance with Article 17 of the GDPR after the request for access had been granted. TF Bank did not deal with the complainant's requests.

TF Bank AB

TF Bank AB states, in essence, as follows. The Bank received and registered the applicant's request for access and erasure on 2 September 2019. Following the commencement of supervision by IMY, the Bank contacted the complainant on 8 December 2023 with information on its internal procedures as well as information on the personal data the Bank holds about the complainant. The complainant's request for erasure was not properly dealt with upon receipt in 2019. Even if the request had been handled, deletion would not have been authorised with reference to the bank's internal procedures at the time of the request and with reference to requirements under anti-money laundering legislation. When a person, at the time of the request, applied for and was approved for any of the bank's products but for some reason chose not to complete the application, the personal data was saved for five years after the bank received information that the application would not be completed. The purpose of the procedure was to prevent fraud, to meet the need to save customer data in order to improve credit approval processes and to meet the requirements of anti-money laundering legislation.

TF Bank AB has also stated that financial information linked to registrants who have not completed their application to become a customer is hidden from the staff of the bank after 90 days from the date that the registrant choose not to complete their application. All other personal data will be irrevocably anonymised after five years. For the complainant, this would take place in September 2024. The bank has now decided to anonymise all customer data linked to the complainant immediately and informed the complainant about it on 8 December 2023. Since 2019, the Bank has implemented improved processes and revised procedures.

Statement by the complainant

At the request of IMY, the German data protection authority gave the complainant the opportunity to comment on the statements made by TF Bank AB. The applicant states, in essence, as follows. It took TF Bank AB four years to respond to the complainant's request. This is an unacceptable delay. Furthermore, the applicant's personal data have not been deleted until more than four years have elapsed. The applicant has suffered significant damage, first, as a result of the unlawful use of his personal data and, second, as a result of the fact that those data were not erased and continued to be processed for four years. If the complainant receives an apology and compensation equivalent to EUR 2 500, he may consider withdrawing his request. Otherwise, the complainant would like a comprehensive supervision to be carried out in order to clarify the matter down to the smallest detail and establish the reasons for the delay.

Reasons for the decision

Applicable provisions

Pursuant to Article 15(1) of the GDPR, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the data and the supplementary information listed in that Article.

Pursuant to Article 17(1) of the GDPR, 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 conditions listed in that Article applies, for example where the data are no longer necessary for the purposes for which they were collected or where consent for processing is withdrawn.

Pursuant to Article 17(3)(b) of the GDPR, the obligation to erase personal data under Article 17(1) does not apply where the processing is necessary for compliance with a legal obligation requiring processing under Union or Member State law to which the controller is subject.

Under Article 12(3) of the GDPR, the controller is to provide the data subject, upon request, without undue delay and in any event no later than one month after receiving the request, with information on the measures taken pursuant to Articles 15 to 22 of the GDPR. This period may be extended in certain circumstances. In such cases, the controller shall inform the data subject of the extension and the reasons for the extension within one month of receipt of the request.

Under Article 82(1) of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the GDPR is entitled to receive compensation from the controller for the damage suffered.

Under Article 79(2) of the GDPR, proceedings against a controller are to be brought before the courts of the Member State in which the controller has an establishment. Alternatively, such proceedings may be brought before the court of the Member State in which the data subject has his or her habitual residence.

Banks are subject to the rules in the Swedish Money Laundering and Terrorist Financing (Prevention) Act (SFS 2017:630), the Swedish anti money laundering, AML, act. Chapter 3, Section 1 of the Swedish AML Act states that an operator may not establish or maintain a business relationship if the operator does not have sufficient knowledge of customers to be able to manage the risk of money laundering or terrorist financing that may be associated with the customer relationship and to monitor and assess the customer's activities and transactions. Chapter 3, Section 4 of the Swedish AML Act states that the operator must take customer due diligence measures when establishing a business relationship. Chapter 5, Section 2 of the Swedish AML Act states that an operator must keep documents and information relating to measures taken for customer due diligence in accordance with Chapter 3 for five years.

The Privacy Protection Authority's assessment

On the basis of the complaints in the case, IMY has examined the company's conduct in the individual case. The review covered the complainant's requests for access under Article 15 GDPR, the complainant's requests for erasure under Article 17 GDPR and

whether the requests were dealt with within the time limit provided for in Article 12(3) GDPR.

With regard to the complainant's request for an apology and compensation of EUR 2 500, IMY notes that it is not within the competence of the authority to decide on compensation to data subjects. The complainant can claim damages by contacting the data controller or by bringing an action for damages in court.

TF Bank AB has informed IMY that it has now granted access to the appellant's data. TF Bank AB also informed IMY that it has now irrevocably anonymised the appellant's data. IMY finds no reason to question that this has happened. IMY notes that TF Bank AB has thus now complied with the complainant's right of access and the complainant's right to erasure. IMY then has to take a position on whether the complainant's request for access or erasure has been handled in a timely manner, and whether TF bank AB has provided information on the measures taken, in response to the request for erasure, in a timely manner.

Has the company dealt with the complainant's request for access in a timely manner pursuant to Article 12(3) of the GDPR?

Pursuant to Article 12(3) of the GDPR, a controller shall handle a request for access pursuant to Article 15 of the GDPR without undue delay and at the latest within one month of receipt of the request. The complainant states that he requested access to his data on 2 September 2019 and that the bank complied with the complainant's request for access on 8 December 2023, following the commencement of supervision by IMY. The request for access was therefore handled four years and three months after the complainant made the request.

IMY therefore finds that TF Bank AB has processed the complainant's personal data in breach of Article 12(3) of the GDPR by failing to comply with the applicant's request for access under Article 15 of the GDPR without undue delay, or at least within one month.

Has the company dealt with the complainant's request for erasure in a timely manner?

TF Bank AB states that, even if they had dealt with the complainant's request for erasure when they received it, they would not have been able to erase the data in the light of internal procedures. The purpose of the procedures was to prevent fraud, to meet the need to save customer data in order to improve credit approval processes and to meet the requirements of anti-money laundering legislation.

Chapter 5, Section 2 of the Swedish AML Act states that an operator must keep documents and information relating to customer due diligence measures taken pursuant to Chapter 3 of the same Act for five years. As a bank, TF Bank AB is subject to the rules of the Swedish AML Act. TF Bank AB can therefore, on the basis of the Swedish AML Act, process the complainant's personal data for five years after customer due diligence measures have been taken. TF Bank AB complied with the complainant's request for erasure after four years and three months. IMY therefore finds that TF Bank AB did not process the complainant's personal data in breach of Article 17 by not deleting the data when the complainant requested it.

Has the company provided the complainant with information in response to the request for erasure in a timely manner pursuant to Article 12(3) of the GDPR?

Pursuant to Article 12(3) of the GDPR, a controller must provide the data subject with information on the action taken in response to a request for erasure pursuant to Article

17 of the GDPR without undue delay and at the latest within one month of receipt of the request.

The complainant states that he requested the erasure of his data on 2 September 2019 and that the bank complied with the complainant's request for erasure on 8 December 2023, following the commencement of supervision by IMY. At the same time, information has been provided in response to the request. Information on the actions taken on the request has thus been provided four years and three months after the complainant made the request.

IMY therefore finds that TF Bank AB has processed the complainant's personal data in breach of Article 12(3) of the GDPR by failing to inform the complainant without undue delay, or at the latest within one month, of the actions taken in response to the complainants's request for erasure under Article 17 of the GDPR.

Choice of corrective measure

It follows from Article 58(2) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines under Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions or prohibitions. Furthermore, it is clear from Article 83(2) which factors must be taken into account when deciding on an administrative fine and when determining the amount of the fine. In the case of a minor infringement, as set out in recital 148, instead of imposing a fine, IMY may issue a reprimand pursuant to Article 58(2)(b). Account shall be taken of aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and relevant previous infringements.

IMY has found that TF Bank processed the complainant's personal data in breach of Article 12(3) of the GDPR. IMY notes the following relevant facts. The infringements found have occurred relatively far back in time. Furthermore, the company has put in place improved processes and revised procedures since the complainant made his request. The Company has not previously received any corrective action for violation of data protection regulations. The complainant's right of access has now been granted and information on the measures taken in response to the request for erasure has been provided. The request for deletion has also been complied with. In those circumstances, IMY finds that the infringements are minor. In view of the fact that the company exceeded the time limit laid down in Article 12(3) of the GDPR by four years and two months, IMY nevertheless considers that, in the context of an overall assessment, there are grounds for giving TF Bank AB a reprimand under Article 58(2)(b) of the GDPR for the infringements found.

28 June 2024 IMY gave TF Bank AB the opportunity comment on a draft decision in accordance with the decision above. TF Bank AB has not commented on the draft decision.

Annex

Complainant's personal data

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

COMPLAINANT

See appendix

CONTROLLER

Aktiebolaget trav och galopp

Swedish ref.:
IMY-2023-16453**Austrian ref.:**
D130.865**IMI case register:**
372595**Date:**
2024-12-19

Final decision under the General Data Protection Regulation – Aktiebolaget Trav och Galopp

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Aktiebolaget Trav och Galopp (ATG, 556180-4161) has processed the complainant's personal data in breach of Article 6 and 7(3) of the General Data Protection Regulation (GDPR)¹ by not making it as easy to withdraw as to give consent, and making it more difficult for the complainant to give an informed and freely given consent, by using a misleading design of its cookie banner.

IMY issues a reprimand to ATG pursuant to Article 58(2)(b) of the GDPR for the infringements.

Presentation of the supervisory case

IMY has initiated supervision regarding ATG due to a complaint. The complaint is one of several complaints filed with the European Data Protection Authorities regarding cookies and cookie banners. The complaints mainly concern the design of cookie banners, the placement of cookies and the subsequent processing of personal data after the cookies have been placed on the complainant's browser or device. To facilitate cooperation on these complaints, a 'Cookie Banner Taskforce' was created within the European Data Protection Board.

In view of the cross-border nature of the processing, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authority concerned has been the Austrian Data Protection Authority.

Postal address:
Box 8114
104 20 Stockholm
Sweden**Website:**
www.imy.se**E-mail:**
imy@imy.se**Telephone:**
+46 (8) 657 61 00

The complainant has essentially stated the following.

On 21 May 2021, ATG processed the complainant's personal data in breach of the GDPR because there was no valid consent. Nor has it been possible to refuse cookies in the first layer and the company has thus made it more difficult to refuse the

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).

processing of personal data. The design of the cookie banner has through colour selection, contrast and links also been misleading, which means that it has not been possible to give an informed and freely given consent in accordance with the GDPR. This is also contrary to the principle of transparency and information. In addition, it has not been as easy to withdraw consent as it has been to give consent.

ATG's information that cookies are used on the website (in a so-called cookie banner) has been attached to the complaint.

ATG has essentially stated the following. On 21 May 2021, ATG had consent as the legal basis for the processing. It was possible to refuse cookies and this could be done in the second layer. It was also possible to withdraw the consent. Information about the right to withdraw consent was provided in the second layer. The consent was withdrawn via ATG's cookie policy under the heading "How do I manage the acceptance/rejection of cookies?".

There were some shortcomings in the consent on 21 May 2021, therefore the following were addressed in October 2021. ATG introduced a clear button to refuse cookies instead of a link. Furthermore, the colour and contrast of the buttons were changed. No cookies other than necessary cookies were placed in the visitor's browser before the visitor made an active consent to cookies. ATG has attached pictures of the changes to the cookie banner.

The complainant has been given the opportunity to comment on ATG's statement and has withdrawn the parts concerning the possibility to refuse cookies in the first layer and misleading link design.

ATG has been given the opportunity to comment on the draft decision.

The scope of the case

The Swedish Post and Telecom Authority is the sole competent supervisory authority over the Electronic Communications Act (2022:482), which contains specific requirements for the storage of cookies in terminal equipment or the collection of data from such equipment. However, the personal data processing that takes place after collection, such as analysis or profiling, is subject to the provisions of the GDPR, where IMY is the competent supervisory authority. Against that background, IMY's investigation has been limited to the processing of personal data that took place after the data was collected and the deficiencies stated in the complaint relating to that subsequent processing.

During the handling of the case, the complainant has stated that the parts regarding no possibility to refuse cookies and that ATG makes it difficult for the complainant to withdraw or refuse consent through the use of a misleading link, have now been remedied. IMY also notes that ATG has changed its cookie banner and that there is now a way to refuse cookies in the first layer and that a button is used instead of a link to refuse cookies. IMY therefore finds no reason to investigate this further.

Motivation for the decision

Applicable provisions, etc.

Processing of personal data is only lawful if one of the conditions set out in Article 6 of the GDPR is met. The legal basis in question in the case is consent pursuant to Article 6(1)(a).

Consent is defined in Article 4(11) of the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For consent to be valid, all of these requirements must be met.

Freely given and informed consent

The transparency of the processing of personal data towards the data subject follows from the principle of transparency set out in Article 5(1) of the Regulation. It is in the light of that principle the requirement that consent must be informed should be read.

Recital 42 of the GDPR states that consent should not be regarded as freely given where the data subject has no genuine or free choice or cannot easily refuse or withdraw his or her consent.

The European Data Protection Board (EDPB) guidelines on consent state that there should be a genuine choice and control for data subjects. As a general rule, the GDPR provides that if the data subject has no real choice, feels compelled to consent or will suffer adverse consequences if they do not consent, the consent will not be valid. The guidelines also state that data controllers must design consent solutions that are clear to data subjects.²

The EDPB further considers that the use of a small font size or a colour that does not contrast sufficiently to provide sufficient readability (e.g. slightly grey text colour on a white background) may have a negative impact on users, as the text becomes less visible and users either overlook it or have difficulty reading it.³

Withdraw consent

Article 7(3) of the GDPR provides that, in order for consent to be valid, the data subject must have the right to withdraw his or her consent at any time. Before consent is given, the data subject shall be informed thereof. It should be as easy to withdraw as it is to give consent.

The EDPB Guidelines on consent state that consent does not have to be given and withdrawn in the exact same action, but should be as simple. In practice, when consent is given electronically by a single mouse click, swipe or keystroke, data subjects must be able to withdraw consent just as easily. Where consent is obtained through a service-specific user interface (e.g. via a website or an app), the data subject must undoubtedly be able to withdraw consent via the same electronic interface, as switching to another interface for the sole purpose of withdrawing consent would require an unjustified effort. In addition, the data subject should be able to

² EDPB Guidelines 05/2020 on consent under Regulation (EU) 2016/679, version 1.1, adopted on 4 May 2020, paragraphs 13 and 84.

³ EDPB Guidelines 03/2022 on misleading design patterns in social media platform interfaces: how to recognise and avoid them, Version 2.0, adopted on 14 February 2023 May, paragraphs 51 and 84.

withdraw the consent without difficulty. This means, among other things, that a controller must ensure that it does not cost anything to withdraw consent or that the service is impaired.⁴

The question in the case is whether there was a valid consent to process the complainant's personal data via cookies.

Assessment

ATG provides information that cookies are used on the website in a so-called cookie banner. The banner is displayed, *inter alia*, when the user first enters the website. In the first layer of the cookie banner, as it appeared on 21 May 2021, there were two options to choose from for the data subject, 'Select your cookies' and 'Accept all cookies'. The following assessment is based on this cookie banner on the company's website.

Comparison of consent and withdrawal procedures

The complainant highlights the option of having a permanently hovering icon visible on all pages of the website to withdraw consent. IMY considers that a permanent hovering icon is an option that can meet the condition that it should be as easy to withdraw as to give consent. On the other hand, IMY does not consider that the GDPR requires a specific technical solution that all controllers must use in order to comply with the requirement of Article 7(3). The assessment of whether it is as easy to withdraw as it is to give consent needs to be made in the individual case on the basis of the procedure in question used to give consent. This assessment is in line with the Cookie Banner taskforce report and the EDPB opinion on valid consent.⁵

During the relevant period, when a user visited ATG's website for the first time, the cookie banner appeared immediately. The title of ATG's cookie banner was 'Accept cookies'. There, the user could, at the click of a button, consent to the use of all (non-essential) cookies. Once a user had given their consent in the cookie banner, the cookie banner disappeared and the website could be used. In order to withdraw consent, the data subject had to go to the company's cookie policy, which was located in the footer under the heading 'Personal data'. There you had to click on the "Cookies" button and then on the "How do I manage the acceptance/rejection of cookies?" button. Information about accepting/denying cookies came up and at the bottom was the option 'click here to open the cookie-settings'. There, the data subject had to click again and then enter a settings center where he or she had to uncheck the categories of cookies to which he or she had previously consented and then press 'save settings'. Thus, when comparing the way consent was obtained on the website, much fewer keystrokes were needed to give consent than to withdraw consent. IMY further considers that it was difficult for a data subject to find where to withdraw consent at all.

Since 21 May 2021, ATG has implemented changes to its cookie banner. Among other things, ATG has added clarification headings on withdrawal under the button 'how do I manage the acceptance/rejection of cookies?' in the cookie policy. However, the data subject still needs to go through all the steps described above in order to withdraw.

⁴ EDPB Guidelines 05/2020 on consent under Regulation (EU) 2016/679, version 1.1, adopted on 4 May 2020, paragraphs 113-114.

⁵ Report on the work of the EDPB Working Group, 'Cookie Banner Taskforce', adopted on 17 January 2023, para. 35 and Opinion 08/2024 on valid consents for "Consent or Pay Models" implemented by large online platforms, adopted on 17 April 2024, paragraph 169 (IMY translation).

IMY's assessment is therefore that the changes made have not led to a data subject being able to withdraw his or her consent as easily as giving consent.

Misleading design

IMY does not consider it possible to introduce a general standard regarding the colours and contrasts that a data controller should use in its cookie banner. An assessment of a cookie banner and whether it complies with the GDPR needs to be made on a case-by-case basis. The assessment shall consider whether contrast and colour are clearly misleading for the data subject and do not result in unintentional and therefore invalid consent. This assessment is in line with the Cookie Banner taskforce report.⁶

IMY does not consider that the option to refuse and to accept cookies needs to look exactly the same in order to comply with the GDPR's provisions on consent. However, they must be equivalent in order for the data subject not to be misled in their choice.

During the period in question, ATG used two different colours for the 'Select your cookies' and 'Accept all cookies' options. For the option not to accept cookies a link was used and for accepting cookies a button was used. The link consisted of grey/black text and the button to approve was green with white text. The background of the banner was white. The option of not accepting cookies, i.e. the link, is therefore not perceived as prominent as a green button on a white background. Furthermore, it is not clear that the link constitutes a possible choice for a user. It seems more like information because the text "Choose your cookies" is designed in the same way as the general information about cookies in the banner. IMY therefore considers that the design of the cookie banner reinforced the perception that the user should click to accept cookies. This must also be seen in the light of the fact that the cookie banner had the heading 'Accept cookies'. IMY considers that ATG's design of the cookie banner and the choice of colours and contrasts were designed to encourage the data subject to accept cookies. ATG has stated that the company needs to comply with regulations to improve accessibility. IMY does not consider that this justifies the need for the company to highlight the option of accepting cookies.

IMY's assessment is that the complainant's consent cannot have been an expression of its unambiguous wish, since the design made it appear that there were no other options than to consent. The complainant cannot therefore have been considered to have had the opportunity to give an informed and freely given consent.

ATG has changed the design of its cookie banner after the complaint. IMY considers that these changes brought some improvements for the data subject to provide freely given and informed consent. However, IMY believes that despite the changes, the design makes the option to accept all cookies more prominent than refusing. This is because the option to accept cookies still has a stronger contrast to the background than the option to refuse cookies. Against that background, IMY considers that ATG used misleading design in its choice of colour and contrast in its cookie banner, which affects the complainant's ability to give an informed and freely given consent.

Summary

ATG has not made it as easy to withdraw consent as to give it. In addition, the company has used misleading designs in its choice of colour and contrast in the cookie banner, which affected the complainant's ability to give an informed and freely

⁶ Report on the work of the Cookie Banner Taskforce, adopted on 17 January 2023, para. 17.

given consent. There was therefore no valid consent and consequently no legal basis for processing the complainant's personal data. ATG therefore processed the complainant's personal data in breach of Article 6 and Article 7(3) of the GDPR.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case need to be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. IMY has assessed that the company has not had a legal basis to process the complainants' personal data. Although ATG is not considered to have made the withdrawal as easy as the giving of consent, there has been an opportunity to withdraw consent and the company has made some improvements after the complaint to make it easier for the data subject. ATG has also made some improvements to the design of the cookie banner, although these have been considered insufficient. The company has not previously been found to have infringed the GDPR.

Against this background, IMY considers these minor infringements within the meaning of recital 148 and that ATG is to be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

COMPLAINANT

See appendix

CONTROLLER

Pierce AB

Swedish ref:
IMY-2022-6646**IMI case register:**
331357**Date:**
2024-12-20

Final decision pursuant to Article 60 under the General Data Protection Regulation

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Pierce AB (556763 – 1592) has processed the complainant's¹ personal data in breach of:

- article 6(1) of the General Data Protection Regulation (GDPR)² by during the period April 7, 2021 – June 6, 2021 having used the complainants email address for the purpose of sending newsletters to him without being able to demonstrate a legal basis for that processing,
- article 13 by having provided the complainant with insufficient information about the processing in question, and
- article 12(3) by not having handled the complainant's request for access on May 30, 2021 without undue delay.

IMY issues a reprimand to Pierce AB pursuant to Article 58(2)(b) of the GDPR for the infringements.

Presentation of the supervisory case

IMY has initiated supervision regarding Pierce AB ('Pierce', the company) due to a complaint. The complaint was submitted to IMY as the lead supervisory authority pursuant to Article 56 of the GDPR. The submission of the complaint was made by the supervisory authority with which the complaint was lodged (the Norwegian supervisory authority) to be handled in accordance with the provisions of the GDPR on cooperation in cross-border processing. In handling the case, IMY has used the cooperation and consistency mechanism of chapter VII of the GDPR. The other supervisory authorities concerned have been the authorities of Austria, Belgium, the Czech Republic, Denmark, Finland, France, Germany, Ireland, Italy, the Netherlands, Norway, Poland and Spain.

Postal address:
Box 8114
104 20 Stockholm**Website:**
www.imy.se**E-mail:**
imy@imy.se**Telephone:**
08-657 61 00

¹ The complainant's identifications data are set out in annex.

² 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).

The complainant has essentially stated the following. After he made a purchase from Pierce on 7 April 2021, and provides his email address, the company sent him marketing emails (newsletters) in large quantities and without legal basis. At the time of purchase, he had neither consented to, nor been given the opportunity to object to, the sending of newsletters. At the time of purchase, he also received insufficient information about the company's processing of his personal data for the purpose of sending newsletters, including no information about the processing of his personal data in connection with the opening and reading of the newsletters. On 30 May 2021, he requested access to his personal data pursuant to Article 15 of the GDPR, to which the company did not respond. The mailings ended a week after his access request. In support of the complaint, the complainant submitted, i.a. written information from the company.

IMY has initiated supervision to investigate whether Pierce had a legal basis pursuant to Article 6(1) of the GDPR to use the complainant's email address to send marketing emails to the complainant during the period in question, whether the complainant has received sufficient information about the processing pursuant to Articles 12 and 13 when the email address was collected, and whether the company handled the complainant's request for access without undue delay. The examination of the case is limited to what the complainant has stated about Pierce's processing of his personal data relating to the newsletters in question, and his request for access on May 30, 2021, and not the company's processing in general. The case has been handled through written procedure.

Pierce has stated that the company is the controller concerning the processing to which the complaint relates.

Reasons for the decision

Legal basis

The lawfulness of the processing of personal data requires a legal basis in Article 6(1) of the GDPR. Personal data can be processed on the basis of a balance of interests under Article 6(1)(f), if the processing is necessary for the purposes of legitimate interests and the interests of the data subject do not override those interests.

Marketing is, according to recital 47 of the GDPR, an example of a purpose that may support the processing of personal data based on a balance of interests. When assessing whether a processing operation can be based on a balance of interests, account may be taken, i.a. of what information the data subject has been given about the processing of his or her personal data, and whether the specific interest may conflict with other legislation, such as the Marketing Act (2008:486).³

Section 19 of the Marketing Act states that, under certain conditions, a trader may use e-mail for marketing to a natural person without consent. One of the conditions is that the natural person, when the e-mail address is collected, is clearly and explicitly given

³ See Recital 70 of the GDPR and EDPB Guidelines 1/2024 on processing of personal data based on Article 6(1)(f), Section 4, adopted for public consultation on October 8, 2024, in particular at paragraph 116.

the opportunity to object to the use of such details for marketing purposes free of charge and easily.

Article 12 of the GDPR imposes a requirement to provide transparent information to the data subject when personal data is collected. Examples of information to be provided pursuant to Article 13 when personal data is collected include the purposes of the processing, the legal basis for the processing and, where the processing is based on Article 6(1)(f), the legitimate interests pursued by the controller or by a third party. In addition, according to the provision, the data subject must be informed at the time of collection of his or her right to object to the processing. Article 21(3) states that the data subject has the right to object to processing for direct marketing purposes. Article 12(2) requires the controller to facilitate the exercise of data subject's rights under Article 21.

The complainant stated that after providing his e-mail address in connection with a purchase from Pierce, he received marketing e-mails (newsletters) from the company without any legal basis. According to the complainant, he had neither consented to, nor been given the opportunity to object to, receiving these mailings.

In the written information from the company, submitted by the complainant in this case, states under the heading *Direct Marketing* that personal data will be used to send offers by e-mail if you have given your consent. Under the headings of *What are your rights* and under *Your right to object to direct marketing*, it is stated that you can opt out of receiving direct marketing by following the instructions in each marketing message.

Pierce has responded to the complaint, including the documents submitted by the complainant in support of the complaint, and mainly stated the following. The company sent approximately 27 e-mail newsletters to the complainant during the period in question. This was done on the basis of a balancing of interests under Article 6(1)(f) of the GDPR. The company does not rely on consent. At the time of the collection, the complainant did not have the opportunity to opt out of receiving e-mail newsletters via a checkbox. In order to be able to send newsletters, the company relies on section 19(2) of the Marketing Act. The company provides the natural person with a clear and simple opportunity to object, free of charge, to the use of their data for marketing purposes both at the time of collection and in each subsequent marketing message. In Pierce's privacy policy, the company informs data subjects of their right to object to direct marketing and how to do so. The data subject could therefore, already at the time of collection, contact the company to opt out of newsletters. Each newsletter sent out also contained a clearly indicated unsubscribe link. The company has now updated its procedures, so that customers are more clearly given the opportunity to decline at the time of collection, and updated its privacy policy, among other things, to be even clearer and comply with the requirements set by IMY and other supervisory authorities in their latest practice. The company has submitted a documented balance of interests that, among other things, refers to Section 19 of the Marketing Act.

IMY notes that the GDPR requires data controllers, when collecting personal data, to provide transparent information on the purposes for which the data will be used and, where applicable, the right to object to the processing, and to facilitate the data subject's right to object to direct marketing.

The investigation shows that when the e-mail address was collected, the complainant was not clearly informed that he would receive marketing e-mails unless he actively

objected. According to the information provided by the company at the time, sending offers by e-mail required his consent. It is questionable whether the procedure was in accordance with Section 19 of the Marketing Act. Against this background, IMY considers that it has not been established that Pierce has been able to rely on Article 6(1)(f) of the GDPR to support the processing of the complainant's personal data in question. No other legal basis has been relevant to apply for the processing. IMY finds that by sending the newsletters in question by email to the complainant without being able to demonstrate a legal basis for the processing, Pierce has processed the complainant's personal data in breach of Article 6(1) of the GDPR.

Information to the complainant

When personal data is collected from a data subject, Article 13 of the GDPR requires the controller to inform the data subject about the processing of his or her personal data.

Some uncertainties in the information provided to the complainant regarding the legal basis and the right to object to the processing has already been taken into consideration when assessing whether the company had a legal basis for sending the newsletter emails to the complainant.

The complainant also claims that the company did not inform him about the processing of his personal data when opening and reading the newsletter.

Pierce has essentially stated the following. Through the company's newsletter register, data has been collected on whether the complainant has opened the newsletters, including whether the complainant has clicked on anything in the newsletters. This information was not previously provided to the complainant, but the company informed the complainant on October 12, 2022 that the company processes information that he has not opened the newsletters. The company has also updated its privacy policy with information about this and referred the complainant to the updated policy.

The investigation shows that, when collecting the complainant's personal data, Pierce did not inform the complainant about the company's processing relating to the complainant's opening and reading of the newsletters in question. IMY finds that by providing insufficient information about the processing of the complainant's personal data at the time of collection, Pierce has processed the complainant's personal data in breach of Article 13 of the GDPR.

Request for access

Pursuant to Article 15 of the GDPR, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, access to the personal data and certain additional information.

Articles 12(3) and 12(4) of the GDPR set out the information to be provided to the data subject in connection to a request for access and the time limits that apply in different cases.

The complainant has stated he requested access from Pierce on May 30, 2021, did not receive a response within one month and when the complaint was filed still had not received a response.

Pierce has essentially stated the following. The complainant's request was not opened because, in accordance with the company's security procedures, the e-mail was unfortunately misinterpreted as a security threat. There was therefore no deliberate refusal of the customer's request, nor was the company unable to handle the request. The complainant's request was granted on 12 October 2022. To minimize the risk of similar situations in the future, Pierce has created an email address for data protection issues, which is referred to in the company's privacy policy.

The investigation shows that the complainant requested access from Pierce on May 30, 2021 and that the company, according to its own statement, did not respond to the request until October 12, 2022.

While there may be circumstances in individual cases that may explain why a request is not opened, controllers have an obligation to take measures to counteract this. One such example is to facilitate, through instructions and guidance, data subjects who wish to exercise their rights. It has not been established that the company had taken sufficient measures in this respect at the time of the request.

IMY finds that by not having handled the complainant's request for access on May 30, 2021, without undue delay, Pierce has processed the complainant's personal data in breach of Article 12(3) of the GDPR.

Choice of corrective measure

In case of infringements of the GDPR, Article 58(2)(i) allows IMY to impose administrative fines in accordance with Article 83. Recital 148 states that in a case of a minor infringement, IMY shall instead issue a reprimand under Article 58(2)(b). In the assessment due regard must be given to the circumstances of each individual case, such as the nature, gravity and duration of the infringement, the scope of the processing, the number of data subjects affected and any relevant previous infringements.

In this case, IMY has taken into consideration the following circumstances. The company has used the complainant's email address for the purpose of sending newsletters without having a legal basis for that processing, provided insufficient information about the processing in question and did not handle the complainant's access request without undue delay. The infringements concern a limited amount of personal data. They do not involve processing of sensitive personal data. There are no previous decisions on infringements of the GDPR against the company. According to the information received, the company has taken actions to remedy the infringements.

Against this background, IMY considers that these are minor infringements within the meaning of recital 148 of the GDPR and that Pierce is to be given a reprimand for the infringements.

This decision has been approved by Head of Unit [REDACTED] after presentation by legal advisor [REDACTED].

[REDACTED]

Appendix

The complainant's personal data

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

CONTROLLER
Kry International AB

Swedish ref.:
IMY-2022-3822

IMI case register:
649079
Date:
2024-12-19

Final decision under the General Data Protection Regulation – Kry International AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Kry International AB (Kry), 556967-0820, has processed personal data in breach of Article 32(1) of the General Data Protection Regulation (GDPR)¹ by not implementing appropriate technical and organisational measures to ensure an appropriate level of security for personal data when using the Meta Pixel during the period May, 28 2020–May 17, 2022.

IMY issues a reprimand to Kry pursuant to Article 58(2)(b) of the GDPR for the infringement.

Presentation of the supervisory case

Background, etc.

On May 18, 2022 Kry notified IMY of a personal data breach. In the notification was inter alia stated that Kry had offered a service used for businesses to businesses in order to facilitate remote contact through a secure and encrypted video connection (the service). The users have typically been healthcare businesses (users) who have been able to register an account and then invite other organisations, colleagues, customers, patients and people representing patients (end-users) by sending out a link to a video meeting by for example text message and email. By using Meta Platforms Ireland Limited's (Meta's) analysis tool the Meta Pixel on the websites where the service was offered, hashed contact information about end-users has been unintentionally transferred to Meta. The incident was discovered by information from a third party.

IMY has initiated supervision in May 2022 in light of the information stated in the notification of personal data breach. The investigation has been limited to the question of whether Kry has implemented appropriate technical and organisational measures in

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

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).

accordance with Article 32 of the GDPR with regard to the processing of the end-users' personal data.

Due to the cross-border nature of the supervisory case, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Denmark, Finland, France, Luxembourg, Netherlands, Norway, Poland, Germany, Hungary and Austria.

Kry's statements

Kry has essentially stated the following with regard to the matter examined in the case.

Controller

Kry is the data controller for the unintentional collection and sharing of end-users' personal data. The implementation of the Meta-pixel has been done by Kry in order to market Kry's own services. Kry has thus determined the purpose and means of the processing in question.

Purpose of the processing

Kry has used the Meta pixel for marketing purposes. The intention has been to collect a limited amount of data about website visitors and users in order to target ads, on Meta's social platform Facebook, to those visitors who have not yet registered an account or users who have registered an account without starting to use the service. The aim was also to evaluate the need and measure the effectiveness of such marketing. Kry has not intended to collect information about or target marketing to end-users. However, due to the activation of the Meta Pixels Automatic Advanced Matching function (AAM function), contact information provided by users about end-users to send out a video meeting invitation has been collected and transferred to Meta. The transmission of the data started on May, 28 2020 and ended on May, 17 2022.

The personal data that has been transferred to Meta

The personal data transferred about the users has included technical information about the users' device, IP address, hashed contact information in the form of email address and phone number, and interaction data such as button presses and events (for example, registration of account, opening of pages or creation of meeting links). The transmission of end-users' contact details has included either their email addresses or telephone numbers. There has been no collection and transmission of data on end-users' use of the service, such as information that the person clicked on a meeting link, joined a meeting or ended a meeting.

It should be noted that several transmitted contact details most likely do not constitute personal data according to the GDPR because they consisted of common email addresses such as info@caretaker.se or switchboard numbers. A review of the pilot project for the service and user feedback further shows that the service was used by healthcare providers inviting a legal entity, such as a health centre or accommodation, as an end-user to the video meeting. In such cases, the contact with the patient has taken place through the legal entity's unit and the booking has not included the processing of the patient's personal data.

The data on end-users did not include special categories of personal data pursuant to Article 9 of the GDPR, inter alia, for the following reasons. It has not been possible to

link data about the end-user to events or actions taken by the user of the service such as invitations or meetings. Meta is very unlikely to have been able to distinguish that the data transferred about the user and the end-user belonged to different parties, since no data suggesting who the data transferred related to was transferred. Activation of the AAM function has resulted in the end-user's email address or phone number being associated with the event instead of the user's email address and phone number. For Meta, it has thus looked like the user changed their contact information. Furthermore, according to the processing agreement that applies between Kry and Meta, Meta has only been allowed to match the contact information with people with accounts on Meta's platforms. Meta has thus also not had the right to try to connect the hashed contact information. Even if Meta could have determined that the data concerned different parties, it has not been possible for Meta to conclude that it was neither a patient nor a caregiver. This would require far-reaching assumptions by Meta as there are many possible links between the different platform accounts other than a healthcare provider and a patient. In addition, the data transferred about users have been professional data and accounts on Meta's platforms are typically of a private nature. It is therefore unlikely that the hashed contact details of the users matched Metas data and Meta has not been able to translate the hashed email address to a readable address.

Scope of the incident

An important principle of the platform and the service has been to not collect, store or otherwise process personal data about end-users. The contact details of the end-users have therefore been deleted from Krys' system immediately after the invitation was sent. For this reason, there are no records or storage of data that can be used to calculate the exact number of unique end-users. Based on the number of calls implemented through the platform and internal statistics from Kry's other services, Kry estimates that approximately 90 000 end-users may have been affected. However, a large part of the contact information of these end-users is unlikely to constitute personal data, which means that the number of data subjects affected by the incident is lower than the reported number.

Krys' investigation also shows that Meta's personal data processing has been limited. The contact details have only, and for a very short period of time, been used to identify Meta's platform users as potential recipients of targeted advertisements and have not been used in any other way. In Sweden, no marketing via Meta was carried out during the period of the incident or afterwards. When Kry became aware of the incident, the pixel was immediately removed from the websites where the service was offered and marketing through Meta was stopped in all markets.

Technial and organisational measures

Kry has taken a number of organisational and technical measures based on the specific risk identified with the processing of personal data within the framework of the service. At the time of the implementation of the service, Kry had internal policies and processes in place. Prior to the commissioning of the service, a risk analysis was carried out, which resulted in an data protection impact assessment. The impact assessment resulted, among other things, in the processing of end-users' personal data being limited to the contact details necessary to send out a meeting invitation. Through data protection by design, Kry has limited as far as possible the extent to which users were able to add data to the system at all. Furthermore, it has been decided that contact data to end-users and other data that needed to be handled in order to provide the service, such as video calls, technical data and metadata about video meetings, would only be processed in real time and thus not saved in Krys'

system. When the marketing department would implement the pixel on the web pages in question, it has not been deemed necessary to carry out another data protection impact assessment because the risks were considered low.

Krys' investigation shows that the technical team that implemented the Meta pixel has not fully understood some of its functionality. Kry has implemented a customer data platform to ensure control over what data that was collected on the websites where the service was offered and to be able to implement overall data protection settings for all tracking. Kry has made a number of settings in the customer data platform to protect personal data, including that no tracking would take place of the end-user page and that directly identified information would be hashed. The AAM function, which caused the unintended transmission, was turned off in the customer data platform for privacy reasons. The incident occurred because opposite settings were made in Meta's own developer tool that was given preference. Since the purpose of the Customer Data Platform is to instruct third-party cookies and pixels, Kry did not foresee that the pixel settings would take precedence over the settings of the Customer Data Platform and thus cause the transfer of personal data. A feature that hashed identified data has been enabled in the customer data platform that allowed the data to be automatically converted from plain text to hashed form. Meta has thus only been given access to hashed personal data. The lack of understanding of the consequences of activating the AAM function, combined with the fact that the technical settings made for the pixel were given precedence over the settings in the customer data platform, thus resulted in hashed contact information to end-users being transferred to Meta even though it was never intended.

Kry applies a principle of minimum privileges, which means that no user role is granted higher privileges than needed to perform its tasks. Only 3–4 people in the marketing department have been able to read and configure the tool for the Meta pixel. The marketing department has continuously and regularly evaluated the statistics regarding the data points and events that the company has decided to collect through the pixel. In addition, an external party has conducted penetration tests of the service on two different occasions. No follow-up of which personal data was collected through the pixel and sent to Meta was done because Kry configured the customer data platform to ensure a limited and secure processing of personal data. Among other things, Kry had taken steps to ensure that no directly identifying personal data from the event data would be shared with Meta. Furthermore, Kry had not understood that the AAM function had been activated and thereby circumvented the privacy settings in the customer data platform form. In May 2022, a more in-depth review of what data was collected and sent to Meta was carried out, which confirmed that some end-user data was mistakenly sent to Meta through the AAM function.

At the time of the incident, Kry has had a general data protection audit programme in place as well as annual internal controls in the field of data protection, based on the requirements of the GDPR and taking into account in particular the risks associated with data processing. However, the risk to the Meta pixel in the context of this programme has been assessed as relatively low, in particular as a result of the target group on which Kry intended to collect data and the measures taken to comply with the applicable legislation. Therefore, it was considered that there was no risk to the AAM function requiring further action as several appropriate measures had already been taken.

When the incident was detected, the Meta pixel was removed from the web pages where the service was offered. Kry has subsequently taken several measures in the

form of, among other things, investigating the incident and informing the data subjects about it on the websites where the service was offered. Kry has also contacted Meta and asked the company to delete the transferred data. Meta informed that all hashed data shared with Meta will be deleted within 48 hours. Kry has also taken steps to improve its handling of tracking technologies. Furthermore, other forward-looking measures have been taken in the form of, for example, reviewing existing requirements and guidelines, training measures and planning the review of functionality in the customer data platform. Kry has not sought or benefited financially from the unintended sharing of data.

Motivation for the decision

IMY will first consider whether the GDPR applies and whether IMY is the competent supervisory authority. If so, IMY will examine whether Kry is the data controller and whether it has implemented appropriate security measures under Article 32 of the GDPR to protect the personal data processed on end-users through the Meta pixel, with the AAM functionality enabled, during the period from May, 28 2020 to May, 17 2022.

IMY's competence

Applicable provisions

It follows from Article 95 of the GDPR that the GDPR shall not impose any additional obligations on natural or legal persons who process personal data, for those areas that are already subject to obligations under the so-called ePrivacy Directive. The ePrivacy Directive has been implemented into Swedish law by the Electronic Communications Act (2022:482) (LEK), which regulates, inter alia, the collection of data through cookies.

Pursuant to Chapter 9, Section 28 of LEK, which implements Article 5(3) of the ePrivacy Directive, data may be stored in or gained from a subscriber's or user's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and consents to it. This does not prevent storage or access which is necessary for the transmission of an electronic message over an electronic communications network or which is necessary for the provision of a service expressly requested by the user or subscriber. The current LEK act entered into force on August, 22 2022. However, during the period in question in this supervisory case, the same requirements applied under Chapter 6, Section 18 of the Electronic Communications Act (2003:389). The Swedish Post and Telecom Authority (PTS) is the supervisory authority under LEK (Chapter 1, Section 5 of Ordinance [2022:511] on electronic communications).

The European Data Protection Board (EDPB) has issued an opinion on the interplay between the ePrivacy Directive and the GDPR. It follows, inter alia, from that opinion that the national supervisory authority designated under the ePrivacy Directive is solely competent to monitor compliance with that directive. However, according to the GDPR, IMY is the competent supervisory authority for the processing that is not specifically regulated in the ePrivacy Directive.²

² Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraphs 68 and 69.

On October, 7 2024 the EDPB adopted guidelines on the technical scope of Article 5(3) of the ePrivacy Directive. The guidelines states, among other things, that a common tool for companies is the use of unique identifiers or persistent identifiers. Such identifiers can be derived from persistent personal data (name, surname, email address, phone number, etc.), which is hashed on the user's device, collected and shared between several controllers to uniquely identify a person through different data sets (user data collected through the use of a website or application, customer relationship management relating to online or offline purchases or subscriptions, etc.). The Guidelines clarify that the fact that the information is entered by the user does not exclude the applicability of Article 5(3) of the ePrivacy Directive, as the information is temporarily stored on the terminal before it is collected. In the case of collection through unique identifiers on web pages or mobile applications, the entity collecting is instructing the browser (through the distribution of client-code) to send that information. As such a gaining of access is taking place and Article 5(3) in the ePrivacy Directive applies.³ The fact that the entity instructing the terminal to send back the information is not the same as the one receiving the information does not exclude the applicability of Article 5(3) of the ePrivacy Directive.⁴

IMY's assessment

The supervisory case is about Krys' use of the Meta-pixel, a script-based tool in the form of a piece of code, on the websites where the service was obtained. The activation of the Meta Pixels AAM function has resulted in the pixel instructing the users' browsers to collect and hash information entered by the users on the website about themselves and the end-user. Based on this data, a unique identifier has been created that is temporarily stored in the user's terminal and then transferred to, and thus gained by, Meta for matching. The processing in question has thus included both storage in and gaining access from the user's terminal equipment referred to in Chapter 9, Section 28 LEK, and the corresponding provision in Chapter 6, Section 18 of the Electronic Communications Act (2003:389).

PTS is solely competent supervisory Authority of the application of the LEK. However, IMY's supervisory case concerns whether Kry has implemented sufficient security measures, which is not specifically regulated in the LEK. IMY is therefore competent to investigate the matter to which the supervisory case relates.

Controller of the processing

Applicable provisions

According to Article 4(7) of the GDPR, the controller is the person who, alone or jointly with others, determines the purposes and means of the processing of personal data. The fact that purposes and means can be determined by more than one actor means that several actors can be controllers for the same processing.

Pursuant to Article 5(2) of the GDPR, the controller must be responsible for and be able to demonstrate compliance with the principles set out in Article 5(1) (principle of accountability).

³ Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, paragraphs 61–63.

⁴ Ibid, paragraph 34.

IMY's assessment

Kry has stated that the company is the data controller for the processing of personal data that the use of the Meta pixel involved and for the transfer of personal data to Meta.

The investigation shows that Kry has decided to introduce the Meta pixel, a tool that tracks website visitors' actions and transmits the information to Meta, on the web pages where the service was offered and then activated the AAM function through the settings in Meta's tool. The purpose of the use of the Meta-pixel has been to promote Kry's service and follow up on this marketing. Kry has therefore decided how the processing should be carried out and for what purpose the personal data should be processed. IMY therefore considers that Kry is the data controller for the processing of personal data that has taken place through the use of the Meta pixel with the AAM function enabled.

Has Kry ensured an appropriate level of security for the personal data?

Applicable provisions

Definition of personal data

According to Article 4(1) of the GDPR, personal data is any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The requirement to implement appropriate security measures

It follows from Article 32(1) of the GDPR that the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by the processing. According to that provision, it must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons. According to Article 32(1), appropriate safeguards include, where appropriate:

- a) pseudonymisation and encryption of personal data;
- b) the ability to ensure the confidentiality, integrity, availability and resilience of processing systems and services,
- c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and
- d) a process for regularly testing, examining and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

Recital 75 of the GDPR sets out factors to be taken into account when assessing the risk to the rights and freedoms of natural persons. It mentions, inter alia, the loss of confidentiality of personal data covered by the obligation of professional secrecy and whether the processing relates to data concerning health or sex life. Account shall also

be taken of whether the processing concerns personal data of vulnerable natural persons, in particular children, or whether the processing involves a large number of personal data and concerns a large number of data subjects.

Recital 76 of the GDPR states that the likelihood and seriousness of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. The risk should be evaluated on the basis of an objective assessment, which determines whether the data processing involves a risk or a high risk.

Data concerning health

Data concerning health belongs to the special categories of personal data, so-called sensitive personal data, which are given a particularly strong protection under the General Data Protection Regulation. As a general rule, the processing of such personal data is prohibited under Article 9(1) of the GDPR, unless the processing is covered by one of the exceptions in Article 9(2) of the GDPR.

Data relating to health are defined in Article 4(15) of the GDPR as personal data relating to the physical or mental health of a natural person which provide information on his or her health status. Recital 35 of the GDPR states that personal data concerning health should include all data relating to a data subject's state of health which provide information on the data subject's past, present or future physical or mental state of health.

IMY's assessment

The process has involved a risk

The controller shall implement measures to ensure a level of protection appropriate with regards to the risks of the processing. The assessment of the appropriate level of protection shall take into account, inter alia, the nature, scope, context and purposes of the processing and the risks, of varying likelihood and severity, to the rights and freedoms of natural persons. On the basis of an objective assessment, it shall be determined whether the processing involves a risk or a high risk.

The investigation in the case shows that Kry has transferred data to Meta about the users of the service in form of, among other things, email address and information about how they acted, for example, in the form of registering an account, opening pages or creating meeting links. Furthermore, the contact details, in the form of email address or phone number, that the user entered about the end-user, in order to create an invitation for a meeting, have been transferred to Meta.

IMY makes the following assessment of the risks associated with the processing of the end-users' personal data.

The kind of data transferred to Meta in the present case may, at least as regards the personal email addresses and telephone numbers, constitutes data capable of directly or indirectly identifying a natural person and thus constitutes personal data. IMY also notes that it cannot be ruled out that it may have been possible to infer from the data transmitted that an invitation to a meeting between the user and the end-user has

been sent. Furthermore, in many cases, it must have been clear from the user's email address that he or she represented a healthcare provider.

However, the transfer in question did not include any information about the relationship between the user and the end-user or any information about what the booking was about. It has thus not been possible to deduce that the end-user was a patient, nor that the meeting constituted a health care visit or what health problems such a visit would concern. IMY therefore considers that the transferred data does not contain any information about the health status of the end-user and thus do not constitute sensitive personal data under the GDPR.

However, given that the service has been used in the healthcare business, IMY notes that the processing, although not involving sensitive personal data on health, has occurred in a context where data subjects must have been able to expect a high degree of confidentiality. This is especially true when the service was used for meetings between a healthcare provider and a patient. In addition, Kry has estimated that up to 90 000 end-users have been affected by the incident.

In conclusion, IMY considers that, having regard to its nature, scope and context, the processing has involved a risk that has required Kry to ensure a level of protection appropriate to the risk in question. Those measures were intended, *inter alia*, to ensure that personal data were protected against loss of control.

Kry has not implemented enough security measurements

IMY shall then assess whether Kry has ensured the level of protection required to protect the end-users' personal data.

Kry has stated that the company made settings in its Customer Data Platform to prevent the use of the Meta pixel's AAM function. However, the company's investigation shows that the function in question has nevertheless been activated because the opposite settings were made in Meta's tool for developers, which was given priority over the settings in the Customer Data Platform. The activation of the AAM feature has resulted in Kry unintentionally transferring end-users' contact information to Meta. However, Kry has taken security measures before the current processing which limited the negative consequences of the unintentional transfer. Among other things, Kry has decided to limit the processing of the end-users' data to what was needed to send out the meeting invitation and implemented technical barriers that prevented the user from entering more data than that. These restrictions have resulted in that it was not possible to read out what the current meeting invitation was about or any other privacy-sensitive information about the data subject.

IMY notes, however, that a basic prerequisite for Kry to be able to fulfill its obligations according to the data protection regulation is that the company is aware of what processing that is taking place under its responsibility. Kry has stated that the company has procedures in place to follow up its processing of personal data. According to the company, however, no follow-up was made of which personal data was collected and transferred to Meta through the pixel, because settings had been made in the customer data platform that would ensure a limited and secure processing of personal data.

For a long period, from May 28, 2020 to May 17, 2022 Kry transferred data about the end-users to Meta that was not intended to be transferred. Only after the company

received information about the incident from a third party did the company carry out investigations that confirmed that such a transfer had taken place. Against this background, IMY assesses that Kry cannot be considered to have had the systematic procedures required to identify such unintentional changes to the processing of personal data as the activation of the Meta-pixel's AAM function entailed. This has meant that Kry lacked control over the treatment and the ability to detect the current deficiency. IMY therefore assesses that Kry, even taking into account the security measures implemented at the time of the breach, cannot be considered to have implemented all the appropriate technical and organisational measures in relation to the risks that the processing has involved. Kry has therefore processed personal data in violation of Article 32 (1) of the GDPR.

Choice of corrective measure

IMY has corrective powers to use against controllers that has violated the GDPR. It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has, inter alia, the power to impose administrative fines in accordance with Article 83 of that regulation. In the case of a minor infringement, IMY may, as stated in recital 148 of the GDPR issue a reprimand pursuant to Article 58(2)(b) instead of imposing an administrative fine. In the assessment IMY should consider aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements.

Kry has processed personal data with an insufficient level of security, which led to an unintentional transfer of personal data relating to a large number of data subjects to Meta. The transfer has been going on for a long time and has not been detected and corrected until a third party informed Kry of the deficiency. The infringement has occurred in a healthcare business where data subjects must be considered to have had a legitimate expectation of a high degree of confidentiality. However, Kry has implemented several measures that have limited the intrusion of the customers' privacy and, among other things, meant that the unintentional transfer did not include data of a privacy-sensitive nature. Furthermore, the measures taken by the company have led to the personal data being transferred in hashed, i.e. illegible, format to a single recipient and it is therefore not an uncontrolled disclosure where, for example, the data has been shared with many unauthorised persons or has been publicly available on the web.

On an overall assessment, IMY considers that this is a minor infringement as referred to in recital 148 of the GDPR and that Kry should therefore be given a reprimand.

This decision has been made by Head of Unit Nidia Nordenström after presentation by legal advisor Maja Welander. The IT- and Information Security Specialist Petter Flink has also participated during the processing of this case.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been

received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

COMPLAINANT

See appendix

CONTROLLER

Svenska Julförlaget AB

Swedish ref.:
IMY-2024-961

Finnish ref.:
7376/153/22

IMI case register:
[598404]

Date:
2024-12-11

Final decision under the General Data Protection Regulation – Svenska Julförlaget AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Svenska Julförlaget AB (Svenska Julförlaget), 556952-143, is processing the complainant's personal data in breach of

- Article 17(1)(c) of the General Data Protection Regulation (GDPR)¹ by not deleting the personal data of the complainant after the complainant has objected to the processing pursuant to Article 21 (2) and
- Article 21(3) of the GDPR by processing the complainant's personal data for direct marketing purposes after the complainant objected to processing for such purposes.

IMY issues a reprimand to Svenska Julförlaget pursuant to Article 58(2)(b) of the GDPR for the stated infringements of the GDPR.

Pursuant to Article 58.2 (c) of the GDPR IMY orders Svenska Julförlaget AB to

- erase the complainant's personal data pursuant to Article 17(1)(c) of the GDPR and
- stop processing the complainant's personal data for direct marketing purposes pursuant to Article 21(3) of the GDPR.

The measures shall be implemented no later than two weeks after this decision has become final.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

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).

Presentation of the supervisory case

The handling of the case

IMY has initiated supervision regarding Svenska Julförlaget AB due to a complaint regarding the right to erasure and objection to direct marketing pursuant to Articles 17 and 21 of the GDPR. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complaint has been lodged (Finland) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authority has been the Finish Authority for Privacy Protection.

The complaint

The complainant has essentially stated the following. Svenska Julförlaget sends sales catalogues to the complainant despite the fact that he has on several occasions asked the company to cease sending him direct marketing and delete his personal data. The direct marketing has continued year after year despite that Svenska Julförlaget has replied that the mailings would stop. According to the complaint the request has, at least, been made in September, 7th 2020 and September, 8th 2021. On August, 25th 2023, the applicant stated that he had again received marketing from Svenska Julförlaget again. Together with the complaint, the complainant submitted a picture of direct marketing from Svenska Julförlaget in the form of a sales catalogue from the year 2022.

When the complainant was given the opportunity to comment on Svenska Julförlaget's statement in the case, as set out below, he also submitted scanned images of Svenska Julförlaget's sales catalogues from 2023 and 2024 and the corresponding sales lists dated 2023 and 2024 showing the appellant's name and address.

Statements from Svenska Julförlaget

Svenska Julförlaget AB has essentially stated the following. Svenska Julförlaget is the controller of the processing of personal data that is the subject to the complaint. Svenska Julförlaget has handled the complainant's request for erasure and objection to direct marketing. The direct marketing in 2020 was sent to the complainant by mistake. In September 2020, the complainant turned to julforlaget.se, but should have emailed julforlaget.fi as it was said that Finnish customers should do for customer service. Since then, the case has not been handled as it should have been, due to the fact that julforlaget.fi was not contacted, and the complainant received incorrect automatic information that the next year's direct marketing would be stopped. The complainant therefore incorrectly received direct marketing in 2021. The complainant emailed the Swedish customer service again in 2021. At that time, attention was paid to the problem and the company introduced a new routine that meant that customer service also handled Finnish customers who emailed to the wrong email address. Svenska Julförlaget buys addresses through an external company. The reason why the complainant could submit a picture of a mailing from 2022 may be that his information was included in the addresses purchased or that he took the mailing from

a neighbour or relative. Nor is it true that the complainant received mailings in 2023 and 2024, since the complainant was removed after his email in 2021 and the customer card was marked 'do not disturb'. The address source is clearly visible from the company's mailings and the address source has been cut from the images submitted by the complainant.

Motivation for the decision

IMY will examine whether Svenska Julförlaget has fulfilled the complainant's request for erasure and whether the company has ceased the processing of the complainant's personal data for direct marketing purposes after he objected to that kind of processing.

Applicable provisions

According to the principle of accountability, the controller must be able to demonstrate that the processing of personal data is carried out in accordance with data protection rules (Articles 5(2) and 24 GDPR). This means that the controller bears the burden of proving that the processing complies with the data protection rules.²

Pursuant to Article 17(1)(c) of the GDPR, the data subject is entitled to have his or her personal data erased by the controller without undue delay, *inter alia*, when the data subject objects to the processing pursuant to Article 21(2) of the GDPR.

Pursuant to Article 21(2) of the GDPR, the data subject has the right to object at any time to processing of personal data concerning him or her for direct marketing purposes. Furthermore, it follows from Article 21(3) of the GDPR, that personal data may no longer be processed for such purposes if a data subject objects to the processing.

IMY:s Assessment

Since 2020, the applicant has repeatedly approached Svenska Julförlaget to request that the company's direct marketing be stopped and that his data should be deleted. IMY considers that the complainant's e-mails should have been interpreted and handled as an objection to direct marketing and the request for erasure.

Svenska Julförlaget has stated that the complainant's email received in 2020 was not handled correctly because he contacted the Swedish customer service department instead of the Finnish one. IMY notes that Svenska Julförlaget has had an obligation to deal with the complainant's request despite that it was sent to an email address that belonged to the company's Swedish customer service. A data subject is not limited to use certain communication channels indicated by the controller as the preferable one, the data subject can also make requests by using other official communication channels of the controller, such as the complainant has done.³

Svenska Julförlaget states that the complainant's request for erasure and objection to direct marketing were dealt with in 2021 and that the company has not sent him any marketing after that date. However, the applicant has submitted documentation in the form of pictures of Svenska Julförlaget's sales catalogues from 2022, 2023 and 2024.

² Dom Valsts ienēmumu dienests, māl C-175/20, EU:C:2022:124 p. 77–81.

³ European data protection Boards (EDPBS) Guidelines 01/2022 on data subject rights – Right of access, p 52–56.

As regards the catalogues of the last two years, the applicant also attached sales lists belonging to the catalogues showing the complainant's name and address. IMY considers that the documentation supports that the complainant has received postal marketing from Svenska Julförlaget in 2022–2024 made for commercial purposes, in order to get him to become a customer of the company, which has been addressed to the complainant. Such mailings constitute direct marketing.⁴ IMY does not consider that the Company has provided any reasonable explanation to disprove that such marketing has been made. IMY considers that the investigation shows that Svenska Julförlaget has processed the complainant's personal data in breach of Article 17(1)(c) by not erasing the complainant's personal data even though he has objected to the processing. IMY also considers that the company has not ceased the processing of his personal data for direct marketing purposes after he objected to it in breach of Article 21(3) of the GDPR.

Choice of corrective measure

In the event of infringements of the General Data Protection Regulation, IMY may direct a number of actions, known as corrective powers, against the subject of supervision. It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has, inter alia, the power to impose administrative fines in accordance with Article 83 of that regulation. In the case of a minor infringement, IMY may, as stated in recital 148 of the GDPR, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements, must be considered.

Svenska Julförlaget has processed the complainant's personal data in breach of Articles 17(1) and 21(3) of the GDPR. However, the infringement in question has affected an individual complainant. Furthermore, the company has not previously been found to have infringed the GDPR.

In the light of the circumstances surrounding the infringements found, IMY considers that these are minor infringements within the meaning of recital 148 and that Svenska Julförlaget should therefore be given a reprimand under Article 58(2)(b) of the GDPR for the breaches.

The investigation in the case shows that the complainant's objection to direct marketing and request for erasure has not been met. IMY therefore considers that it is appropriate to order Svenska Julförlaget pursuant to Article 58(2)(c) to delete the complainant's personal data pursuant to Article 17(1)(c) of the GDPR and to stop processing the complainant's personal data for direct marketing in accordance with Article 21(3) of the GDPR. The measures shall be implemented no later than two weeks after this decision has become final.

This decision has been made by decision maker [REDACTED] after presentation by legal advisor [REDACTED].

⁴ Dom StWL Städtische Werke Lauf a.d. Pegnitzden, mål C-102/20, EU:C:2021:954, p 47.

Appendix
The complainant's personal data

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-05-27, no. DI-2022-222. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2022-222, IMI number:
336110

Date of decision:
2022-05-27

Date of translation:
2022-08-25

Beslut efter tillsyn enligt dataskyddsförordningen – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that Klarna Bank AB has processed personal data in breach of

- articles 12(3) and 17 GDPR¹ by not informing the complainant without undue delay until 17 September 2021 of the measures taken in response to the request for deletion of 16 August 2021; and
- articles 12(3) and 21(2) by not ceasing the processing of personal data of the complainant for direct marketing purposes without undue delay until 9 September 2021, following the objection of 16 August 2021;

The Swedish Integrity Protection Authority gives Klarna Bank AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany, Berlin) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, Ireland, Germany, Poland, Spain, Italy and Finland.

The complaint

The complaint states the following. The complainant has received payment reminders from Klarna following a purchase from Wayfair Inc. The complainant then has (i) objected to Klarna's processing of the applicant's personal data in general and (2)

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

objected to direct marketing and (3) requested the deletion of his personal data.

What Klarna has stated

Klarna has mainly stated the following.

Klarna is the data controller for the processing to which the complaint relates.

Klarna received the objection to direct marketing and the objection to the processing of the complainant's personal data on 16 August 2021. Klarna states that the processing carried out in connection with the direct marketing is based on the legal bases set out in Article 6(1)(e) and (f) of the GDPR. The processing has ceased as of 9 September 2021, except in cases where Klarna has legitimate interests for the processing that outweigh the interests of the complainant, such as fraud prevention in future purchases.

On 9 September 2021, Klarna blocked the complainant from further marketing communications from the company.

Klarna received a request for erasure on 16 August 2021. Following the request, Klarna asked the complainant to provide information to confirm his identity. The complainant did not return to that information. In violation of Klarna's procedures and by error of an employee, erasure of the complainant's personal data has nevertheless started on 17 September 2021 and was completed on 17 October 2021. Due to Klarna's failure to verify the identity of the complainant, the time limit in Article 12(3) of the GDPR has not started to run.

Justification of the decision

Applicable provisions, etc.

According to Article 12(3) of the GDPR, upon request, the controller must comply with the individual's request without undue delay and in any event no later than one month after receiving the request. The period of one month may be extended by a further two months if the request is particularly complex or the number of requests received is high. If the deadline of one month is extended, the controller shall notify the individual of the extension. The extension of the time limit shall be notified within one month of receipt of the request. The controller shall also state the reasons for the delay.

Without prejudice to Article 11, where the controller has reasonable grounds to doubt the identity of the natural person submitting a the request pursuant to Articles 15 to 21, request the provision of additional information necessary to confirm the identity of the individual. This is developed in Article 12(6).

Under Article 17(1)(c), individuals have the right to have their personal data erased without undue delay when they object pursuant to Article 21(1).

Under Article 21(1), the individual shall have the right, on grounds relating to his or her specific situation, to object at any time to processing of personal data concerning him or her based on Article 6(1)(e) (information in the public interest or the exercise of official authority) or (f) (legitimate interest), including profiling based on those provisions. The controller shall no longer process the personal data unless we can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual, or for the establishment, exercise or

defense of legal claims.

Under Article 21(2), the individual always has the right to object to the use of his or her personal data for direct marketing purposes. If the personal data are objected to by way of direct marketing, the personal data shall no longer be processed for such purposes, as follows from Article 21(3).

Article 12(3) requires that a request under Article 21 be dealt with without undue delay and in any event within one month at the latest. That period may be extended by a further two months, if necessary, taking into account the complexity of the request and the number of requests received.

According to the European Data Protection Board's (EDPB) Guidelines 01/2022 on access, the calculation of the one-month deadline in Article 12(3) is calculated from the date of receipt of the request. However, where, upon receipt of the request, a controller needs to take steps to ensure the identity of the data subject, the time limit may be suspended until the controller has received the information necessary to identify the data subject. This is provided that the request for further information has been made without undue delay.¹

Assessment of the Authority for Privacy Protection (IMY)

Has Klarna handled the complainant's objection under Article 21(1) correctly? The investigation into the case shows that the complainant's objection to the processing of personal data was raised on 16 August 2021. Klarna has stated that the company has ceased the processing of personal data based on the legal bases set out in Article 6(1)(e) and (f) on 9 September 2021, except in cases where Klarna has legitimate interest such as fraud prevention in future purchases. IMY finds no reason to question this. The question, therefore, is whether Klarna has done so without undue delay.

The complainant has exercised the right, pursuant to Article 21(1), to object to Klarna's processing of personal data based on Article 6(1)(e) and (f) on grounds relating to his or her specific situation. Since Klarna has not demonstrated the existence of legitimate grounds for the processing, Klarna was obliged to discontinue the processing without undue delay from when the request was received.

Klarna stopped treatment 24 days later. IMY considers that Klarna has ceased to process the complainant's data without undue delay and thus acted in accordance with Article 21(1) and (3) GDPR.

Has Klarna handled the appellant's objection to direct marketing under Article 21(2) correctly?

On 16 August, the complainant objected to direct marketing pursuant to Article 21(2) of the GDPR. Klarna has blocked the complainant from further marketing communications from the company on 9 September 2021.

IMY notes that, by exercising its absolute right under Article 21(2) to object to direct marketing, Klarna has been under an unconditional obligation under Article 21(3) to cease such processing of personal data without undue delay within the meaning of

¹ See EDPB Guidelines 01/2022 on data subject rights — Right of access, Version 1.0, adopted for public consultation on 18 January 2022, (EDPB Guidelines 01/2022 on access), p. 47 f; IMY's translation.

Article 12(3). Since, unlike a request under Article 21(1), there is no room for Klarna to weigh a request under Article 21(2), such a request should be able to be dealt with more hastily. Klarna ceased with the processing 24 days after the objection was received, which IMY finds not to have been without undue delay. Klarna has thus processed the complainant's personal data in breach of Articles 12(3) and 21(2) of the GDPR.

Has Klarna handled the appellant's request for deletion correctly? The investigation shows that the applicant's request for erasure was received by Klarna on 16 August 2021. On 9 September 2021, i.e. 24 days later, Klarna considered it necessary to obtain additional information from the complainant in order to secure the complainant's identity and therefore requested additional information. Since the subject matter of the complaint does not relate to whether it was actually justified to request such information, IMY does not take a position this matter. However, IMY notes that by taking 24 days to request additional information, it cannot be considered to be without undue delay. The deadline for handling the request shall therefore not be considered to have been suspended in the period until Klarna started erasure and informed about it on 17 September 2021.

As regards the fulfilment of the request, Klarna started the erasure on 17 September 2021 and at the same time sent the complainant information about this and the maximum time the erasure could take. The erasure was completed on 15 October 2021, i.e. after 62 days, which IMY considers to have taken place without undue delay.²

However, Klarna informed the complainant of the measures taken only 32 days after the request was received. In those circumstances, IMY considers that Klarna has processed the applicant's personal data in breach of Articles 12(3) and 17 of the GDPR by informing the applicant only on 17 September 2021 of the measures taken in response to the request of 16 August 2021.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The time that has passed before the company acted was relatively short. Nor has it been sensitive or privacy-sensitive data. The requests have now been handled by Klarna and completed. Against this background, IMY considers that these are minor infringements within the meaning of recital 148 and that Klarna Bank AB should therefore be given a reprimand under Article 58(2)(b) of the GDPR for the infringements found.

This draft decision has been approved by the specially appointed decision-maker [REDACTED]
[REDACTED] after presentation by legal advisor [REDACTED]

Copy to

Data Protection Officer [REDACTED]

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision in case with national reference number, DI-2020-11397. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2020-11397

Date of decision:
2023-06-30

Final decision under the General Data Protection Regulation– CDON AB transfers of personal data to third countries

Table of contents

Decision of the Swedish Authority for Privacy Protection (IMY)	3
1. Report on the supervisory case	3
1.1 Processing	3
1.2 What is stated in the complaint	4
1.3 What CDON has stated.....	4
1.3.1 Who has implemented the Tool and for what purpose etc.	4
1.3.2 Recipients of the data.....	5
1.3.3 The data processed in the Tool and what constitutes personal data	5
1.3.4 Categories of persons concerned by the treatment	5
1.3.5 When the code for the Tool is executed and recipients are accessed	5
1.3.6 How long the personal data are stored	5
1.3.7 The countries in which personal data are processed	6
1.3.8 CDON's relationship with Google LLC	6
1.3.9 Ensure that processing is not carried out for the purposes of the recipients	6
1.3.10 Description of CDON's use of the Tool	6
1.3.11 Own checks on transfers affected by the judgment in Schrems II	6
1.3.12 Transfer tools under Chapter V of the GDPR.....	7
1.3.13 Verification of obstacles to compliance in third country legislation	7
1.3.14 What information is covered by the definition of personal data....	7
1.3.15 Effectiveness of measure taken by Google and CDON	8

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

1.4 What Google LLC has stated	8
1.5 CDON's comment on Google's opinion	10
2 Statement of reasons for the decision	10
2.1 The framework for the audit	10
2.2 This is the processing of personal data.....	11
2.2.1 Applicable provisions, etc.....	11
2.2.2 Assessment of the Swedish Authority for Privacy Protection (IMY)	12
2.3 CDON is the data controller for the processing.....	15
2.4 Transfer of personal data to third countries	15
2.4.1 Applicable provisions, etc.....	15
2.4.2 Assessment of the Swedish Authority for Privacy Protection (IMY)	17
3 Choice of intervention	21
3.1 Legal regulation.....	21
3.2 Should an administrative fine be imposed?	21
3.3 Other interventions.....	24
4 How to appeal	25

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that the investigation has shown that CDON AB processed personal data in breach of Article 44 of the GDPR¹ by using the Google Analytics tool provided by Google LLC on its website www.cdon.fi, and thus transferring personal data to third countries without fulfilling the conditions laid down in Chapter V of the Regulation, since 14 August 2020 and until the date of this Decision.

Pursuant to Article 58(2)(d) of the GDPR, CDON AB is required to ensure that the company's processing of personal data in the context of the company's use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V of the GDPR. In particular, CDON AB shall cease to use the version of the Google Analytics tool used on 14 August 2020, unless sufficient safeguards have been taken. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

On the basis of Articles 58(2) and 83 of the GDPR, IMY decides that CDON AB shall pay an administrative fine of SEK 300 000 (three hundred thousand) for infringement of Article 44 of the GDPR.

1. Report on the supervisory case

1.1 Processing

The Swedish Integrity Authority for Protection Authority (IMY) has initiated supervision regarding CDON AB (hereinafter CDON or the company) due to a complaint. The complaint has claimed a breach of the provisions of Chapter V of the GDPR related to the transfer of the complainant's personal data to third countries. The transfer is alleged to have taken place when the complainant visited the company's website, www.cdon.fi (hereinafter "the company's website" or the "Website") through the Google Analytics tool (hereinafter the Tool) provided by Google LLC.

The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Austria) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned are the data protection authorities in Germany, Norway, Estonia, Denmark, Portugal, Spain, Finland and Austria.

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).

1.2 What is stated in the complaint

The complaint has essentially stated the following.

On 14 August 2020 the complainant visited the CDON website. The complainant visited the controller's website, while being logged in to the Google/ Facebook account associated with the complainant's email address. On the website, the controller has embedded a JavaScript code for Google/ Facebook services including "Google Analytics" or "Facebook Connect". In accordance with paragraph 5.1.1(b) of the terms and conditions of Google's processing of personal data for Google's advertising products and also Google's terms and conditions for processing the New Google Ads Processing Terms, for Google Advertising Products, Google processes personal data on behalf of the controller (i.e. CDON) and is therefore to be classified as the company's data processor.

During the visit of the company's website, CDON processed the complainant's personal data, at least the complainant's IP address and the data collected through cookies. Some of the data has been transferred to Google. In accordance with Section 10 of the Terms and Conditions on the Processing of Personal Data for Google's Advertising Products, CDON has authorised Google to process personal data of the Applicant in the United States. Such transfer of data requires legal support in accordance with Chapter V of the GDPR.

According to the judgment of the Court of Justice of the European Union (CJEU), in Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)², the company could no longer rely on an adequacy decision under Article 45 of the GDPR for the transfer of data to the United States. CDON should not base the transfer of data on standard data protection clauses under Article 46(2)(c) GDPR if the recipient of the personal data in the third country does not ensure appropriate protection with regard to Union law for the personal data transferred.

Google shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881 (4)(b) and is thus subject to surveillance by U.S. intelligence services in accordance with 50 US § 1881a (Section 702 of the Foreign Intelligence Surveillance Act, below "702 FISA").³ Google provides the U.S. government with personal data in accordance with these provisions. CDON cannot therefore ensure adequate protection of the complainant's personal data when it is transmitted to Google.

1.3 What CDON has stated

CDON AB have in opinions on the 15 January 2021, 15 February 2022 and 31 August 2022, essentially stated the following.

1.3.1 Who has implemented the Tool and for what purpose etc.

The code for the Tool was embedded on the Website at the time of the complaint and is still embedded on the Website. The decision to embed the Tool on the Website was made by CDON, a company registered in Sweden. Data is collected from all persons

² Judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

³ See <https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm> and <https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881a.htm>.

visiting the Website, which is likely to include data subjects from more than one EU/EEA Member State.

CDON uses the Tool to get to know the traffic and uses the Website to make various business-critical decisions. It is possible to find out which product categories are most popular and how customers navigate, partly to find CDON and to end a purchase.

1.3.2 Recipients of the data

In the context of CDON's use of the Tool on the Website, personal data is only disclosed to Google.

1.3.3 The data processed in the Tool and what constitutes personal data

The data processed in the context of CDON's use of the Tool are different characteristics or actions taken by the visitor on the Website, such as:

1. What elements the user has seen while navigating and looking around the Site,
2. Clicked on an Image/Banner on the Website,
3. Added or removed something to the cart,
4. Came to checkout or completed a purchase,
5. Clicked on suggestions for accessories on product pages or added something to the wishlist,
6. If the user is a member of the CDON customer club; and
7. The search string used by the user to search internally on the Website.

In addition to this data, Google also has access to the IP address of the respective user.

1.3.4 Categories of persons concerned by the treatment

The categories of persons concerned by the processing are all categories of persons who visit the Website. CDON has no means of distinguishing if data on particularly vulnerable persons are processed. This is because CDON only processes anonymous "behavioural data" regarding how a user navigates the Website. The information processed by CDON is no more than the transfer of the information to Google. CDON cannot identify individual users before or after disclosure to Google. The category of persons a unique user belongs to is therefore unknown to CDON.

1.3.5 When the code for the Tool is executed and recipients are accessed

Immediately after the Website has finished loading into the user's browser, information about the location of the user on the Website has been transmitted to Google. Since 12 January 2021, CDON has activated a tool that requires the respective user's consent to integrate and run the content of the Tool into the user's browser.

1.3.6 How long the personal data are stored

Data and other information are not stored by CDON, but are transmitted by CDON to Google in real time. CDON's assessment is that the anonymisation of IP addresses described below means the data transferred to Google can no longer be linked to a specific individual and are therefore not personal data. Google will only store personal

data until the IP addresses are truncated⁴. According to Google, truncation is executed as soon as technically possible.

1.3.7 The countries in which personal data are processed

The data transmitted to the Tool is stored, for example in the United States.

1.3.8 CDON's relationship with Google LLC

CDON share the assessment made by Google regarding the allocation of personal data, whereby Google is deemed to process data in the context of CDON's use of the Tool as a data processor for CDON. CDON acts as data controller.

The terms that apply to the tool are both Google's Terms of Service and Google's data processing terms.

The sharing of personal data by Google and CDON is set out in the Google Ads Data Processing Terms.

1.3.9 Ensure that processing is not carried out for the purposes of the recipients

CDON has not had any reason to assume that Google does not meet the requirements of the Google Ads Data Processing Terms, so that its compliance with those terms has not yet been further verified by CDON.

1.3.10 Description of CDON's use of the Tool

CDON uses the Tool in order to get to know the traffic on the Website and to be able to make various business-critical decisions based on that information. For example, it is possible to find out which product categories are most popular and how customers navigate the Website to find CDON and to end a purchase.

1.3.11 Own checks on transfers affected by the judgment in Schrems II

Following the Schrems II judgment, CDON has taken measures in the form of identifying which of CDON's partners are located in countries outside the EU/EEA and, in relation to the respective partners, requested information on the additional security measures they have taken as a result of the ruling.

On October 26, 2020, CDON requested information from Google regarding the effect of CDON's embedding of the Code for the Tool on the Website. Google has not returned in response to CDON's request for information and, for this reason, in addition to repeating the request to Google and reminding of replies, CDON has sought publicly available information on the actions taken by Google as a result of the ruling.

According to publicly available information from Google, in addition to the Standard Contractual Clauses, Google has taken the following additional safeguards in relation to the Tool:

- Google ensures the secure transfer of JavaScript libraries and measurement data using the HTTP HSTS (Strict Transport Security) encryption protocol.
- The Tool has been certified according to the internationally accepted independent safety standards ISO 27001.

⁴ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

In addition to these actions, CDON has also chosen to activate IP anonymisation in the code of the tool, which means that IP addresses are truncated. IP anonymisation means that the last octet of IPv4 addresses and the last 80 bits of IPv6 addresses are deleted immediately after the addresses have been sent to the Tool Collection Network. Since CDON's view is that it is the IP addresses that cause the other data collected and transmitted using the Tool to be considered personal data, CDON's assessment is that the truncation of the IP addresses means that no information transmitted to Google is considered personal data after the IP anonymisation/trunking has been carried out.

1.3.12 Transfer tools under Chapter V of the GDPR

Transfers of personal data to recipients in third countries under CDON's use of the Tool are carried out on the basis of the European Commission's Standard Contractual Clauses (2010/87/EU).

In accordance with the versions of Google's data processing terms in force since 12 August 2020, Google and CDON have entered into EU Standard Contractual Clauses for the transfer of data from an EU controller to a data processor outside the EU, based on template 2010/87/EU of the European Commission.

1.3.13 Verification of obstacles to compliance in third country legislation

In order to ensure compliance with the contractual obligations set out in the standard contractual clauses, CDON has sent the request for information to Google regarding third country transfer described above and CDON has received no reply.

1.3.14 What information is covered by the definition of personal data

It is important to distinguish between the concepts of being able to distinguish users and not being able to identify a specific individual. The latter, identification of a specific individual is not the purpose of the use of the Tool, nor is it possible with the information collected by unique identifiers (which may be derived from the browser or device (i.e. CDON's Google Analytics account ID)) neither alone nor in combination with, *inter alia*, the information generated during visits to the Website (i.e. Web address (URL) and HTML title on that Website or browser information). CDON is of the firm opinion that IP addresses are necessary to process, among other things, the information generated when visiting the Website (i.e. URL (URL) and HTML title on that Website or information about browsers) may be considered personal data. CDON acknowledges that in certain circumstances dynamic IP addresses may be considered personal data. However, the differentiation of users made possible by the information collected by unique identifiers is not sufficient for a specific individual to be identified, with or without means such as, for example, disclosure, but only in combination with a full IP address that the information collected by unique identifiers and information generated by visits to the Website may constitute personal data.

The judgments Breyer⁵ and M.I.C.M.⁶ support the assessment that dynamic IP addresses are, in all cases, personal data. According to the Court of Justice, dynamic IP addresses may be regarded as personal data in relation to the provider of information or communication services concerned, not in relation to any operator accessing an IP address. In the judgement Breyer, concerning the assessment of the means which could reasonably be used to identify the person concerned, the Court held that, under German law, there were legal means enabling the provider of

⁵ Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:C:2016:779.

⁶ Judgment of the Court of Justice of the European Union M.I.C.M., C-597/19, EU:C:2021:492.

electronic information or communications services, in particular in the event of cyber attacks, to apply to the competent authority in order to take the necessary steps to obtain such information from the internet service provider and to initiate criminal proceedings. It may be questioned whether a U.S. authority with a truncated IP address, which may constitute one of 256 alternative IP addresses, has such lawful means as may reasonably be used to enable the identification of an individual, when, in the case of Breyer, a full IP address was even considered problematic in relation to the actual provider of that natural person's IT services.

1.3.15 Effectiveness of measure taken by Google and CDON

With reference to the answers above, in addition to the activation of IP anonymisation, CDON has not considered the implementation of accompanying measures as Google has informed that additional measures have been taken.

The truncation of IP addresses is an effective protection measure. Regardless of whether the IP addresses are truncated in connection with, or in connection with, the transmission of the information from CDON to Google. The truncation of the IP addresses means that the information stored on Google's servers in the United States does not constitute personal data. In a situation where the truncation takes place only after the data has been received by Google LCC, but at the latest immediately after receipt, the truncation means that all the data transmitted by CDON to Google and stored on Google's servers will not constitute personal data because the IP address, which is the unique identifier that causes the other information transmitted to constitute personal data, has been anonymised. The IP address without the last octet may be any of 256 alternative IP addresses and therefore a truncated IP address by thinning together with other information cannot be considered personal data.

1.3.16 Supplementary measures taken in addition to those taken by Google

During the handling of the case, CDON has thoroughly analysed and investigated the possibilities of switching to another solution that does not involve the use of the Tool. CDON have done preparations for such a change, which it will hopefully be able to implement promptly if IMY's final decision indicates that the Tool is not compliant with the GDPR and when that kind of decision becomes final. CDON's analysis shows that such a change (i.e. switch to a different solution) will be very burdensome for the company (in particular in comparison with other market players), so that it cannot be implemented before there is clarity in relation to what applies to the Tool as to what is a supplementary measure.

1.4 What Google LLC has stated

IMY has added to the case an opinion of Google LLC (Google) on 9 April 2021 submitted by Google to the data protection authority in Austria. The opinion answers questions asked by IMY and a number of regulators to Google in response to partial joint handling of similar complaints received by these authorities. CDON has been given the opportunity to comment on Google's opinion. Google's opinion shows the following about the Tool.

A JavaScript code is included on a web page. When a user visits (calls) a web page, the code triggers a download of a JavaScript file. After that, the Tool tracking operation, which consists of collecting information related to the call in different ways and sending the information to the server of the Tool, is performed.

A website manager who integrated the Tool on his website may send instructions to Google for the processing of the data collected. These instructions are transmitted via the so-called tag manager who manages the tracking code that the webmaster has integrated into his website and through the tag manager's settings. The person who integrated the tool can make different settings, for example regarding storage time. The Tool also enables those who integrated it to monitor and maintain the stability of their website, for example by keeping themselves informed of events such as peaks in visitor traffic or lack of traffic. The Tool also enables a website manager to measure and optimise the effectiveness of advertising campaigns carried out using other Google tools.

In this context, the Tool collects visitor's http calls and information about, among other things, the visitor's browser and operating system. According to Google, a http call for any page contains information about the browser and device making the call, such as domain names, and information about the browser, such as type, reference and language. The Tool stores and reads cookies in the visitor's browser to evaluate the visitor's session and other information about the call. Through these cookies, the Tool enables unique users identification (UUID) over browsing sessions, but the Tool cannot identify unique users in different browsers or devices. If a site owner's website has its own authentication system, the site owner can use the ID feature to identify a user more accurately on all the devices and browsers they use to access the site. When the information is collected, it is transferred to the servers of the Tool. All data collected through the Tool is stored in the United States.

Google has put in place, among other things, the following legal, organisational and technical measures to regulate transfers of data within the framework of the Tool.

Google has put in place legal and organisational measures, such as that it always conducts a thorough review of a request for access from government authorities if user data can be implemented. It is lawyers/specially trained staff who conduct these trials and investigate whether such a request is compatible with applicable laws and Google's guidelines. Data subjects are informed of the disclosure, unless prohibited by law or would adversely affect an emergency. Google has also published a policy on its website on how to implement such a request for access by government authorities of user data.

Google has put in place technical measures such as protecting personal data from interception when transmitting data in the Tool. By default using HTTP Strict Transport Security (HSTS), which instructs browsers such as http to SSL (HTTPS) to use an encryption protocol for all communication between end-users, websites, and tool servers. Such encryption prevents intruders from passively listening by communications between websites and users.

Google also uses encryption technology to protect personal data known as "data at rest" in data centers, where user data is stored on a disk or backup media to prevent unauthorised access to the data.

In addition to the above actions, website owners may use IP anonymisation by using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated and contribute to data minimisation. If the IP anonymisation service is fully used, the anonymisation of the IP address takes place almost immediately after the request has been received.

Google also restricts access to the data from the Tool through permission control and by all personnel having completed information security training.

1.5 CDON's comment on Google's opinion

CDON maintains what was stated in the opinion of 15 January 2021. In addition, CDON presents the following in response to Google's opinion of 9 April 2021.

In its use of the Tool, CDON has taken the security measures provided by the Tool.

Google's observations state, *inter alia*, as follows:

"As a general matter, unless instructed to do so, Google does not attempt to link data it collects as a processor on behalf of website owners using Google Analytics with data it collects as a controller in relation to its users and the relevant policies and systems are designed to avoid such linking."

Google thus states that the owner of the website has full control over the personal data processed by Google by allowing users of the tool to provide Google with specific instructions to link the personal data with users. CDON has not given Google any such instructions.

CDON has instead focused on using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated. CDON had also limited the storage time of the personal data and has not enabled the User ID function. CDON has thus not been able to link a fixed ID of a single user to the user's engagement data from one or more sessions initiated from one or more devices.

In conclusion, CDON maintains that the use of the Tool has been carried out in accordance with the security measures offered by the Tool. It should also be noted that obligations under Chapter V of the GDPR are primarily obligations imposed on the exporter, which in this case are CDON resellers (see EDPB Guidelines 05/2021 and decisions of the data protection authority in Austria regarding Google Analytics in case 2021-0.586.257 (D155.027)).

2 Statement of reasons for the decision

2.1 The framework for the audit

Based on the complaint in the case, IMY has only examined whether CDON transfers personal data to the third country USA within the framework of the Tool and whether CDON has legal support for it in Chapter V of the GDPR. The supervision does not cover whether CDON's personal data processing otherwise complies with the General Data Protection Regulation.

2.2 This is the processing of personal data

2.2.1 Applicable provisions, etc.

In order for the GDPR to apply, personal data must be processed.

According to Article 1(2), the GDPR aims to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. According to Article 4(1) of the GDPR personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In order to determine whether a natural person is identifiable, account should be taken of all means which, either by the controller or by another person, may reasonably be used to directly or indirectly identify the natural person (recital 26 of the GDPR).

That concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject. As regards the latter condition, it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person.⁷

The word "indirectly" in Article 4(1) of the GDPR suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.⁸ In addition, recital 26 of the GDPR states that in order to determine whether a natural person is identifiable, any means, such as 'singling out', which, either by the controller or by another person, may reasonably be used to directly or indirectly identify the natural person, should be taken into account. In order to determine whether devices *may reasonably be used to* identify the natural person, all objective factors, such as the cost and duration of identification, taking into account both the available technology at the time of processing, should be taken into account. According to Article 4 (5) of the GDPR, 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

So-called "net identifiers" (sometimes referred to as "online identifiers") — e.g. IP addresses or information stored in cookies — can be used to identify a user, especially when combined with other similar types of information. According to recital 30 of the GDPR, natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses, cookies or other identifiers. This may leave traces that, in particular in combination with unique identifiers and other data collected, can be used to create profiles of natural persons and identify them.

In its Breyer judgment, the Court of Justice of the European Union held that a person is not regarded as identifiable by a particular indication of whether the risk of

⁷ Judgment of the Court of Justice of the European Union Nowak, C-434/16, EU:2017:994, paragraphs 34-35.

⁸ Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:2016:779, para. 41.

identification is in practice negligible, which is whether the identification of the person concerned is prohibited by law or impossible to implement in practice.⁹ However, in the judgment in M.I.C.M. of 2021 and in the Breyer judgment, the Court of Justice of the European Union held that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.¹⁰

2.2.2 Assessment of the Swedish Authority for Privacy Protection (IMY)

In order to determine whether the data processed through the Tool constitute personal data, IMY shall decide whether Google or CDON, through the implementation of the Tool, can identify individuals, e.g. the complainant, when visiting the Website or whether the risk is negligible.¹¹

IMY considers that the data processed constitute personal data for the following reasons.

The investigation shows that CDON implemented the Tool by inserting a JavaScript code (a tag), as specified by Google, into the source code of the Website. While the page loads in the visitor's browser, the JavaScript code is loaded from Google LLC's servers and runs locally in the visitor's browser. A cookie is set simultaneously in the visitor's browser and stored on the computer. The cookie contains a text file that collects information about the visitor's operation on the Website. Among other things, a unique identifier is set in the value of the cookie and this unique identifier is generated and managed by Google.

When the complainant visited the Website, or a subpage of the Website, the following information was transmitted via the JavaScript code from the complainant's browser to Google LLC's servers:

1. Unique identifier(s) that identified the browser or device used to visit the Website and a unique identifier that identified CDON (i.e. the CDON account ID for Google Analytics).
2. URL and HTML title of the website and web page visited by the complainant;
3. Information about browser, operating system, screen resolution, language setting, and date and time of access to the Website.
4. The complainant's IP address.

At the time of the complainant's visit, the identifiers referred to in paragraph 1 above were set in cookies with the names '_gads', '_ga' and '_gid' and subsequently transferred to Google LLC. Those identifiers were created with the aim of distinguishing individual visitors, such as the complainant. The unique identifiers thus make visitors to the Website identifiable. However, even if such unique identifiers (according to 1 above) were not in themselves to make individual identifiable, it must be borne in mind that, in the present case, those unique identifiers may be combined with additional elements (according to paragraphs 2 to 4 above) and that it is possible

⁹ Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:2016:779, paragraphs 45-46.

¹⁰ Judgment of the Court of Justice of the European Union M.I.C.M. C-597/19, EU:2021:492, para. 102-104, and Breyer, C-582/14; EU:C:2016:779, paragraph 49.

¹¹ See the Administrative Court of Appeal in Gothenburg's judgment of 11 November 2021 in case No 2232-21, with the agreement of the lower court.

to draw conclusions in relation to information (as set out in paragraphs 2 to 4 above) from which data constitute personal data, irrespective of whether the IP address was not transmitted in its entirety.

Combined data (according to points 1-4 above) means that individual visitors to the Website become even more separable. It is therefore possible to identify individual visitors to the Website. This in itself is sufficient for it to be considered personal data. Knowledge of the actual visitor's name or physical address is not required, as the distinction (by the word 'release' in recital 26 of the GDPR, 'singling out' in the English version) is sufficient in itself to make the visitor indirectly identifiable. Nor is it necessary for Google or CDON to identify the complainant, but the possibility of doing so is in itself sufficient to determine whether it is possible to identify a visitor. *Objective means that can reasonably be used* either by the controller or by another, are *all means that can reasonably be used* for the purpose of identifying the complainant. Examples of *objective means that can reasonably be used* are access to additional information from a third party that would allow the complainant to be identified taking into account both the available technology at the time of identification and the cost (time required) of the identification.

IMY notes that, in its judgments in M.I.C.M. and Breyer, the Court of Justice of the European Union held that dynamic IP addresses constitute personal data in relation to the person processing them, where it also has a legal means to identify the holders of internet connections using the additional information available to third parties.¹² IP addresses do not lose their character of being personal data simply because the means of identification lie with third parties. The Breyer judgment and the M.I.C.M. judgment should be interpreted on the basis of what is actually stated in the judgments, i.e. if there is a lawful possibility of access to additional information for the purpose of identifying the complainant, it is objectively clear that there is a '*legal means which enable it*' to identify the complainant. According to IMY, the judges should not be read in contrast, in such a way as to demonstrate a legally regulated possibility of access to data that could link IP addresses to natural persons in order for the IP addresses to be considered personal data. In IMY's view, an interpretation of the concept of personal data which implies that there must always be a *legal possibility* of linking such data to a natural person would constitute a significant restriction on the area of protection of the Regulation and would open up the possibility of circumventing the protection provided for in the Regulation. That interpretation would, *inter alia*, run counter to the objective of the Regulation as set out in Article 1(2) of the GDPR. The Breyer judgment is decided under Directive 95/46 previously in force and the notion of 'singling out' as set out in recital 26 of the current regulation (not requiring knowledge of the actual visitor's name or physical address, since the distinction itself is sufficient to make the visitor identifiable), was not mentioned in the previous directives as a means of identifying personal data.

In this context, there are also other data (according to paragraphs 1 to 3 above) with which the IP address can be combined to enable identification. Google's action regarding¹³ the truncation of an IP address means that the IP address can still be

¹² Judgment of the Court of Justice of the European Union M.I.C.M, C-597/19, EU:2021:492, para. 102-104 and Breyer, C-582/14

EU:C:2016:779, paragraph 49.

¹³ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this action means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.

distinguished as it can be linked to other data transmitted to third countries (to the United States). This enables identification, which in itself is sufficient for the data to constitute personal data together.

In addition, several other supervisory authorities in the EU/EEA have decided that the transfer of personal data to third countries has taken place in the use of the Tool because it has been possible to combine IP addresses with other data (according to paragraphs 1 to 3 above), thus enabling the separation of data and the identification of the IP address, which in itself is sufficient to determine the processing of personal data.¹⁴

IMY notes that there may also be reasons to compare IP addresses with pseudonymised personal data. In accordance with Article 4(5) of the GDPR, pseudonymisation of personal data means that the data — like dynamic IP addresses — can no longer be attributed to a specific data subject without the use of additional information. According to recital 26 of the GDPR, such data should be considered to be data relating to an identifiable natural person.

According to IMY, a narrower interpretation of the concept of personal data would undermine the scope of the right to the protection of personal data, as guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, as it would allow controllers to specifically designate individuals together with personal data (e.g. when they visit a particular website) while denying individuals the right to protection against the dissemination of such data. Such an interpretation would undermine the level of protection of individuals and would not be compatible with the broad scope of the data protection rules laid down in the case-law of the Court of Justice of the European Union.¹⁵

Furthermore, CDON, by being logged in to its Google account when visiting the Website, processed data from which it was able to draw conclusions about the individual on the basis of his registration with Google. Google's opinion shows that the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a data subject) has visited the website in question. It is true that Google states that certain conditions must be met in order for Google to receive such information, such as that the user (applicant) has not disabled the processing and display of personal ads. Since the applicant was logged in to its Google account when visiting the Website, Google may still have been able to obtain information about the logged-in user's visit to the Website. The fact that it is not apparent from the complaint that no personalised ads have been displayed does not mean that Google cannot obtain information about the logged-in user's visit to the Website.

In the light of the unique identifiers CAPABILITY of identifying the browser or device, the ability to derive the individual through its Google account, the dynamic IP addresses and the possibility of combining these with additional data, CDON's use of the Tool on a website, means the processing of personal data.

¹⁴ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

¹⁵ See, for example, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:2021:504, paragraph 61; Nowak, C-434/16, EU:2017:994, paragraph 33; and Rijkeboer, C-553/07, EU:2009:293, paragraph 59.

2.3 CDON is the data controller for the processing

The controller is, among other things, the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4(7) GDPR). The processor is, among other things, a legal person who processes personal data on behalf of the controller (Article 4(8) GDPR).

The responses provided by CDON indicate that CDON has made the decision to implement the Tool on the Website. It also appears that CDON's purpose was to enable the company to analyse how the Website is used, in particular to be able to monitor the use of the website over time.

IMY finds that CDON, by deciding to implement the Tool on the Website for that purpose, has determined the purposes and means of the collection and subsequent transfer of this personal data. CDON is therefore the data controller for this processing.

2.4 Transfer of personal data to third countries

The investigation shows that the data collected through the Tool is stored by Google LLC in the United States. Thus, the personal data collected through the Tool is transferred to the United States.

The question is therefore whether CDON's transfer of personal data to the United States is compatible with Article 44 of the GDPR and has legal support for it in Chapter V.

2.4.1 Applicable provisions, etc.

Article 44 of the GDPR, entitled 'General principle for the transfer of data', provides, *inter alia*, that transfers of personal data which are under processing or are intended to be processed after their transfer to a third country — i.e. a country outside the EU/EEA — may take place only if, subject to the other provisions of the GDPR, the controller and processor fulfil the conditions set out in Chapter V. All provisions of that chapter are to be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

Chapter V of the GDPR contains tools that can be used for transfers to third countries to ensure a level of protection that is essentially equivalent to that guaranteed within the EU/EEA. This could include, for example, transfers based on an adequacy decision (Article 45) and transfers subject to appropriate safeguards (Article 46). In addition, there are derogations for specific situations (Article 49).

In Schrems II, the Court of Justice of the European Union annulled the adequacy decision previously in force in respect of the United States.¹⁶ In the absence of an adequacy decision since July 2020, transfers to the United States cannot be based on Article 45 of the GDPR.

Article 46(1) provides of the GDPR, *inter alia*, that in the absence of a decision in accordance with Article 45(3), a controller or processor may only transfer personal data to a third country after having taken appropriate safeguards, and subject to the

¹⁶ 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 Privacy Shield of the European Union and the United States and the judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

availability of statutory rights of data subjects and effective remedies for data subjects. Article 46(2)(c) provides that such appropriate safeguards may take the form of standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).

In Schrems II, the Court of Justice did not reject standard contractual clauses as a transfer tool. However, the Court found that they are not binding on the authorities of the third country. In that regard, the Court held that '*Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.*'¹⁷

The reason why the Court of Justice of the European Union annulled the adequacy decision with the US was how the U.S. intelligence agencies can access personal data. According to the Court of Justice, the conclusion of standard contractual clauses cannot in itself ensure a level of protection required by Article 44 of the GDPR, as the safeguards set out therein do not apply when such authorities request access. The Court of Justice of the European Union therefore stated:

*'It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.'*¹⁸

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgment¹⁹ clarify that if the assessment of the law and practice of the third country means that the protection guaranteed by the transfer tool cannot be maintained in practice, the exporter must, in the context of his transfer, as a rule either suspend the transfer or take appropriate supplementary measures. In that regard, the EDPB notes that '*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it - by itself or in combination with others - addresses the specific deficiencies identified in your assessment of the situation in the third country as regards its laws and practices applicable to your transfer. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.*'²⁰

¹⁷ Points 125-126.

¹⁸ Paragraph 133.

¹⁹ 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 (hereinafter "EDPB Recommendations 01/2020").

²⁰ EDPB Recommendations 01/2020, item 75.

The recommendations of the EDPB show that such supplementary measures can be divided into three categories: contractual, organisational and technical.²¹

As regards *contractual* measures, the EDPB states that such measures "*In some situations, these measures may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country*" [...]. Provided the nature of contractual measures, generally not capable of binding the authorities of that third country when they are not party to the contract, these measures may often need to be combined with other technical and organisational measures to provide the level of data protection required [...]."²²

With regard to *organisational* measures, the EDPB stresses "[a] electing and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. Depending on the specific circumstances of the transfer and the assessment performed on the legislation of the third country, organisational measures are needed to complement contractual and/or technical measures, in order to ensure a level of protection of the personal data essentially equivalent to that guaranteed within the EEA".²³

With regard to *technical* measures, the EDPB points out that 'measures, which may supplement safeguards found in Article 46 GDPR transfer tools to ensure compliance with the level of protection required under EU law in the context of a transfer of personal data to a third country'.²⁴ The EDPB states in this regard that "The measures listed below are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. These measures would be necessary to guarantee an essentially equivalent level of protection to that guaranteed in the EEA, even if the public authorities' access complies with the law of the importer's country, where, in practice, such access goes beyond what is necessary and proportionate in a democratic society.⁷⁹ These measures aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts".²⁵

2.4.2 Assessment of the Swedish Authority for Privacy Protection (IMY)

2.4.2.1 Applicable transfer tool

The investigation shows that CDON and Google have entered into standard data protection clauses (standard contractual clauses) within the meaning of Article 46 for the transfer of personal data to the United States. These clauses are in line with those published by the European Commission in Decision 2010/87/EU and thus a transfer tool under Chapter V of the GDPR.

²¹ EDPB Recommendations 01/2020, item 52.

²² EDPB Recommendations 01/2020, item 99.

²³ EDPB Recommendations 01/2020, item 128.

²⁴ EDPB Recommendations 01/2020, item 77.

²⁵ EDPB Recommendations 01/2020, item 79.

2.4.2.2 Legislation and situation in the third country

As can be seen from the judgment in Schrems II, the use of standard contractual clauses may require supplementary measures. Therefore, an analysis of the legislation of the third country in question needs to be carried out.

IMY considers that the analysis already carried out by the Court of Justice of the European Union in Schrems II, which relates to similar circumstances, is relevant and topical, and that it can therefore serve as a basis for the assessment in the case without further analysis of the legal situation in the United States.

Google LLC, as an importer of the data to the United States, shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881(b)(4). Google is therefore subject to surveillance by U.S. intelligence agencies pursuant to 50 US § 1881a (“702 FISA”) and is therefore obliged to provide the U.S. government with personal data when 702 FISA is used.

In Schrems II, the Court of Justice of the European Union held that the US surveillance programmes based on 702 FISA, Executive Order 12333 (hereinafter ‘E.O. 12333’) and Presidential Policy Directive 28 (hereinafter ‘PPD-28’) do not meet the minimum requirements laid down in EU law in accordance with the principle of proportionality. This means that the monitoring programmes based on those provisions cannot be considered to be limited to what is strictly necessary. In addition, the Court found that the monitoring programmes do not confer rights on data subjects that may be invoked against US authorities in court, which means that those persons do not have the right to an effective remedy.²⁶

Against this background, IMY notes that the use of the European Commission’s standard contractual clauses is not in itself sufficient to achieve an acceptable level of protection for the transferred personal data.

2.4.2.3 Supplementary measures implemented by Google and CDON

The next question is whether CDON has put in place supplementary measures.

As the controller and exporter of the personal data, CDON is obliged to ensure compliance with the rules of the GDPR. This responsibility includes, *inter alia*, assessing, on a case-by-case basis, in the case of transfers of personal data to third countries, which supplementary measures are to be used and to what extent, including assessing whether the measures taken together by the recipient (Google) and the exporter (CDON) are sufficient to achieve an acceptable level of protection.

2.4.2.3.1 Google’s supplementary measures

Google LLC, as an importer of personal data, has taken contractual, organisational and technical measures to supplement the standard contractual clauses. In its opinion of 9 April 2021, Google stated that it had taken action.

The question is whether the supplementary measures taken by CDON and Google LLC are effective, in other words, hindering the ability of U.S. intelligence agencies to access the transferred personal data.

²⁶ Paragraphs 184 and 192. Paragraph 259 et seq.

As regards the *legal and organisational measures*, it can be noted that neither information to users of the Tool (such as CDON), the²⁷ publication of a transparency report or a publicly available “government enquiries policy” prevents or reduces the ability of U.S. intelligence services to access the personal data. In addition, it is not described what it means that Google LLC’s “scrupulous review” of any “legality” request from U.S. intelligence agencies. IMY notes that this does not affect the legality of such requests as, according to the CJEU, they are not compatible with the requirements of EU data protection rules.

As regards the *technical measures* taken, neither Google LLC nor CDON have clarified how the described measures — such as the protection of communications between Google services, the protection of data when transferring between data centres, the protection of communications between users and websites, or “physical security” — prevent or reduce the ability of U.S. intelligence services to access the data under the US regulatory framework.

With regard to the encryption technology used — for example, for so-called “data at rest” (“data at rest”) in data centers, which Google LLC mentions as a technical measure — Google LLC as an importer of personal data nevertheless has an obligation to grant access to or supply imported personal data held by Google LLC, including any encryption keys necessary to make the data understandable.²⁸ Thus, such a technical measure cannot be considered effective as long as Google LLC is able to access the personal data in plain language.

As regards Google LLC’s argument that ‘*to the extent that data for measurement in Google Analytics transmitted by website holders constitute personal data, they may be regarded as pseudonymised*’, it can be concluded that Universal Unique Identifiers (UUIDs) are not covered by the concept of pseudonymisation in Article 4(5) of the GDPR. Pseudonymisation can be a privacy-enhancing technology, but the unique identifiers, as described above, have the specific purpose of distinguishing users and not serving as protection. In addition, individual identification is made through what has been stated above about the ability to combine unique identifiers and other data (e.g. metadata from browsers or devices and the IP address) and the ability to link such information to a Google account for logged-in users.

In the case of Google’s “anonymisation of IP addresses” in the form of truncation²⁹, Google’s response does not indicate whether this action takes place prior to transmission, or whether the full IP address is transmitted to the United States and shortened only after transmission to the United States. From a technical point of view, it has therefore not been shown that there is no potential access to the entire IP address before the last octet is truncated.

Against this background, IMY concludes that the supplementary measures put in place by Google are not effective, as they do not prevent US intelligence services from accessing the personal data or rendering such access ineffective.

²⁷ Regardless of whether such a notification would even be permitted under U.S. law.

²⁸ See EDPB Recommendations 01/2020, paragraph 81.

²⁹ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

2.4.2.3.2 CDON's own supplementary measures

CDON has stated that it has taken supplementary measures in addition to the measures taken by Google. According to the CDON, these consist of activating the function of truncating³⁰ the last octet of the IP address before the data is transmitted to Google, which means that the last octet is masked.³¹

As stated above with regard to Google's actions, it is not apparent from Google's reply whether this action takes place prior to transmission or whether the full IP address is transmitted to the United States and truncated only after the transfer to the United States. Therefore, from a technical point of view, it has not been established that, after the transmission, there is no potential access to the entire IP address before the last octet is truncated.

Even if the truncation were to take place before the transfer, it is not a sufficient measure, as the truncated IP address can be linked to other data, as IMY stated above in section 2.2.2. A truncation of an IP address means that only the last octet is masked, which in itself can only be any of 256 options (i.e. in the range 0-255) and because the truncated IP address can be distinguished from other IP addresses, this data can be linked to other data (as described in section 2.2.2) and enable identification, which is sufficient in itself to determine whether the data is a personal data. Although the masking of the last octet constitutes a privacy-enhancing measure, as it limits the scope of the data that authorities can access (in third countries), IMY notes that it is nevertheless possible to link the transferred data to other data which are also transferred to Google LLC (in third countries).

Against this background, IMY also notes that the supplementary measures taken by CDON in addition to the supplementary measures taken by Google are not effective enough to prevent US intelligence services from accessing the personal data or rendering such access ineffective.

2.4.2.3.3 Conclusion of the Swedish Authority for Privacy Protection (IMY)

IMY finds that CDON and Google's actions are neither individually nor collectively effective enough to prevent U.S. intelligence services from accessing the personal data or rendering such access ineffective.

Against this background, IMY considers that neither standard contractual clauses nor the other measures relied on by CDON can support the transfer as set out in Chapter V of the GDPR.

With this transfer of data, CDON therefore undermines the level of protection of personal data for data subjects guaranteed by Article 44 of the GDPR.

IMY therefore concludes that CDON AB violates Article 44 of the GDPR.

³⁰ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

³¹ See above in the section on CDON's submissions, under the heading 'Supplementary protective measures taken'.

3 Choice of intervention

3.1 Legal regulation

In case of breaches of the GDPR, IMY has a number of corrective powers available under Article 58(2)(a) to (j) of the GDPR, including reprimand, injunctions and administrative fines.

IMY shall impose fines in addition to or in place of other corrective measures referred to in Article 58(2), depending on the circumstances of each case.

Each supervisory authority shall ensure that the imposition of administrative fines on a case-by-case basis is effective, proportionate and dissuasive. This is set out in Article 83(1) of the GDPR.

Article 83(2) of the GDPR sets out the factors to be taken into account in determining whether an administrative fine is to be imposed, but also in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand under Article 58(2)(b) of the Regulation. Account must be taken of aggravating and mitigating circumstances in the case, such as the nature, gravity and duration of the infringement and the relevant past infringements.

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR, which aim to create a harmonised methodology and principles for the calculation of fines.³²

3.2 Should an administrative fine be imposed?

IMY has found above that the transfers of personal data to the United States carried out through the Google Analytics tool and for which CDON is responsible are contrary to Article 44 of the GDPR. Infringements of that provision may, in accordance with Article 83, impose fines.

Given, among other things, that CDON has transferred a large amount of personal data, that the processing has been going on for a long time and that the transfer has meant that the personal data could not be guaranteed the level of protection afforded in the EU/EEA, this is not a minor breach. A fine must therefore be imposed on CDON for the infringement found. See also below under 3.3 for a detailed description of the gravity of the infringement.

3.2.1 To what amount should the administrative fine be determined to?

In determining the maximum amount of a fine to be imposed on an undertaking, the definition of ‘undertaking’ used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR). It is clear from the Court’s case-law that this applies to any entity engaged in an economic activity, irrespective of its legal form and the way in which it is financed, and even if, in the legal sense, the entity consists of several natural or legal persons.³³

³² EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

³³ See judgment in Akzo Nobel, C-516/15, EU:C:2017:314, paragraph 48

Pursuant to Article 83(5)(c) GDPR, in the event of infringement of, inter alia, Article 44 in accordance with 83(2), administrative fines of up to EUR 20 million or, in the case of an undertaking, up to 4 % of the total global annual turnover in the preceding financial year, whichever is higher, are to be imposed.

IMY considers that the company's turnover to be used as a basis for calculating the administrative fine is CDON's annual report for 2022. The company had sales of approximately SEK 461 000 000 during that financial year. This amount is less than EUR 20 million and the administrative fine can therefore be set at an amount of up to EUR 20 million.

In determining the amount of the fine, IMY shall determine, having regard to the gravity of the infringement and taking into account both aggravating and mitigating factors, an administrative fine amount which is effective, proportionate and dissuasive in the individual case.

IMY considers that the following factors are relevant to the assessment of the gravity of the infringement.

As far as the assessment of the gravity of the infringement is concerned, there are, at the outset, factors that lead to a more serious assessment of the infringement. CDON is transferring a large amount of personal data to third countries. The transfer has meant that the personal data have not been guaranteed the level of protection afforded in the EU/EEA, which in itself is a serious breach. In addition, it is aggravating that the transfer of personal data has been going on for a long time, i.e. from 14 August 2020 and is still ongoing, and that it has taken place systematically. IMY also takes into account that it has now elapsed around 3 years since the Court of Justice of the European Union, by judgment of 16 July 2020, rejected the Commission's adequacy decision in the United States,³⁴ thereby changing the conditions for transfers of personal data to the United States.

In the meantime, the EDPB made recommendations on the consequences of the judgment that had been put out for public consultation on 10 November 2020 and adopted in final form on 18 June 2021. In addition, several other EU/EEA supervisory authorities have issued injunctions to discontinue the use of the Tool until sufficiently effective security measures have been taken by the controllers. The decisions have covered cases where the controllers have also taken measures such as the "anonymisation of IP addresses" in the form of truncation.³⁵

Although these recommendations and decisions clearly point to the risks and difficulties of ensuring an adequate level of protection for data transfers to U.S. companies, CDON has not put in place supplementary measures of its own. Google's³⁶ IP truncation action means that the IP address can still be distinguished as

³⁴ 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-US Privacy Shield.

³⁵ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

³⁶ Truncation of IP address "anonymisation of IP address" means that asterisks or zeros replace other digits in last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this measure means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information about the entity and time of visit) to third countries (to the USA).

it can be linked to other data transmitted to third countries (to the United States). This enables identification, which means that the data together constitute personal data.

The CDON website is also a well-attended e-commerce portal that offers goods from many different suppliers and is available in several countries and in several languages. These are data on a large number of data subjects in the EU/EEA that can be identified indirectly and whose data can be linked to other data relating to them. As regards the nature of the data, it follows from CDON's own purpose of processing — i.e. to be able, *inter alia*, to draw conclusions on how data subjects navigate and find the Website, that the data taken together make it possible to draw relatively precise conclusions about the privacy of data subjects and to map them, such as what they buy and which goods they are interested in over time. CDON's analysis of the Tool shows that the company have a proposal for a solution other than the Tool, but the company has chosen not to introduce this solution due to the fact that such a change would be particularly burdensome for the company. CDON's processing of personal data entails obvious risks of serious violation of the rights and freedoms of individuals, which gives CDON a special responsibility which imposes high standards in the case of transfers to third countries, where IMY overall considers that CDON has not demonstrated that it has carried out sufficient analysis and mapping, nor has it taken the necessary security measures to limit the risks to the data subjects.

At the same time, IMY notes that there are factors that speak in the opposite direction. IMY takes into account the specific situation arising after the judgment and the interpretation of the EDPB's recommendations, where there has been a gap after the transfer tool to the United States has been rejected by the Court of Justice of the European Union, according to the Commission's previous decision. IMY also takes into account that CDON has taken some, albeit insufficient, measures to restrict the personal data transmitted by activating the "anonymisation of IP addresses" by truncation.³⁷ That fact is also taken into account when assessing the gravity of the infringement.

Overall, considering the facts set out in this decision, IMY considers that the infringements in question are of a low degree of seriousness. The starting point for calculating the fine should therefore be set low in relation to the maximum amount in question. In order to ensure a proportionate fine in the individual case, it is also necessary, at this stage, to further adjust the starting point for the further calculation downward, taking into account the high turnover underlying the calculation of the fine.

In addition to assessing the gravity of the infringement, IMY shall assess whether there are any aggravating or mitigating circumstances that have a bearing on the amount of the fine. IMY considers that there are no additional aggravating or mitigating circumstances, other than those taken into account when assessing the severity, which affect the amount of the fine.

On the basis of an overall assessment of the above facts and in the light of the fact that the administrative fine must be effective, proportionate and dissuasive, IMY considers that the fine may remain at SEK 300 000 (three hundred thousand).

³⁷ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

3.3 Other interventions

Against this background IMY considers that CDON should be ordered pursuant to Article 58(2)(d) of the GDPR to ensure that its processing of personal data in the context of its use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, by discontinuing the use of the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards are in place. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

4 How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

This decision was taken by Director-General [REDACTED] following a presentation by the legal advisor [REDACTED]. [REDACTED], Head of Legal Affairs, [REDACTED], Head of Unit and information security specialist [REDACTED]. [REDACTED] have also participated in the final proceedings.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's draft decision in case with national reference number, DI-2019-11737. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2019-11737

Date:
2023-06-26

Decision under the General Data Protection Regulation –Bonnier News AB

Content

1. Decision of the Authority for Privacy Protection	3
2. Presentation of the supervisory case	3
2.1 Description of the group common processing of personal data	4
2.1.1 Description of the processing of personal data contained in the behavioural database	5
2.1.2 Description of the processing of personal data stored in KDB	6
3. Statement of reasons for the decision	8
3.1 IMY's competence	8
3.1.1 Circumstances at issue	8
3.1.2 Applicable provisions, etc	8
3.1.3 IMY assessment	9
3.2 Bonnier News AB's responsibility for the data processing	9
3.2.1 Circumstances at issue and Bonnier News AB's position	9
3.2.2 Applicable provisions, etc	9
3.2.3 IMY assessment	10
3.3 What constitutes personal data?	10
3.3.1 Circumstances at issue and Bonnier News AB's position	10
3.3.2 Applicable legal provisions other legal sources	11
3.3.3 IMY's position	12
3.4 The processing constitutes profiling	13
3.4.1 Applicable provisions	13
3.4.2 IMY's position	13
3.5 Legal basis for processing for the purpose of displaying personalised advertisements based on data in the behavioral database	13
3.5.1 Circumstances at issue and Bonnier News AB's position	13

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

3.5.2 Applicable provisions, etc.....	15
3.5.3 Basic principles for IMY's assessment.....	17
3.5.4 Legitimate interest.....	19
3.5.5 Is the processing necessary for the legitimate interest?	19
3.5.6 Balancing test test for the processing of personal data in supplemented behavioural profiles	19
3.5.7 Balance of interests for the processing of personal data in simple behavioural profiles	21
3.6 Legal basis for processing for the purpose of making contact information available for telemarketing and postal direct marketing.....	22
3.6.1 Applicable provisions, etc.....	22
3.6.2 Circumstances at issue and Bonnier News AB's position.....	22
3.6.3 IMY's assessment.....	24
3.6.4 Legitimate interest.....	24
3.6.5 Is the processing necessary for the legitimate interest?	24
3.6.6 Balance of interests for the processing of personal data in supplementary customer database profiles	24
3.6.7 Balance of interests for personal data not linked to the behavioural database	25
3.7 Choice of corrective measure	26
3.7.1 Applicable provisions etc.....	26
3.7.2 Same or interconnected data processing operations.....	26
3.7.3 Administrative fine.....	27

1. Decision of the Authority for Privacy Protection

The Swedish Authority for Privacy Protection notes that Bonnier News AB during the period from 7 November 2019 to 11 June 2020 has processed personal data without having a lawful basis pursuant to Article 6(1) of the GDPR¹ by:

- a) processing personal data for the purpose of profiling the data subjects based on their behavioural data in so-called supplemented behavioural profiles and making those profiles available to affiliated companies for the purpose of displaying targeted advertisements;
- b) processing personal data for the purpose of profiling the data subjects based on their behavioural data in so-called simple behavioural profiles and making those profiles available to affiliated companies for the purpose of displaying targeted advertisements;

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).

- c) processing personal data by profiling the data subjects based on their supplemented customer database profiles in order to make contact information available to affiliated companies for telemarketing and postal marketing;

Pursuant to Articles 58(2) and 83 of the GDPR, the Swedish Authority for Privacy Protection decides that Bonnier News AB shall pay an administrative fine of SEK 13 000 000 (thirteen million).

2. Presentation of the supervisory case

In a supervision of Bonnier Magazine and Brands AB (ref. DI-2019-6523), the Swedish Authority for Privacy Protection (IMY) has found that Bonnier News AB, together with other companies within the Bonnier Group, processes personal data for, amongst other, marketing purposes based on the lawful basis legitimate interest pursuant to Article 6(1)(f) of the GDPR. IMY has initiated supervision against Bonnier News AB in order to investigate whether Bonnier News AB complies with the GDPR requirements for the processing of personal data that takes place for marketing purposes.

Within the framework of the supervision, Bonnier News AB has been given the opportunity to give its opinion on seven complaints addressed to IMY concerning various marketing measures taken by companies within the Bonnier Group of companies.² According to Bonnier News AB those marketing actions mentioned in the complaints have not happened due to withdrawals from the group wide/group common databases. Bonnier News AB has therefore stated that they are not the controller for the processing of the complainants' personal data regarding marketing. In the light of the above, IMY does not find it appropriate to further investigate these complaints within the context/scope of this supervision/case.

Within the scope of the supervision, IMY has examined whether Bonnier News AB has a lawful basis pursuant to Article 6 of the GDPR for the processing of personal data in the group-wide/group common databases for marketing purposes. The supervision covers the processing of personal data conducted through creating profiles and making it available to affiliated companies to be used to display personalized advertisements. It also covers the processing of personal data, the creation of profiles and the making available of data to affiliated companies in order to be used by affiliated companies in telemarketing and postal direct marketing. IMY has not taken a position on whether Bonnier News AB's personal data processing otherwise complies with the General Data Protection Regulation.

The supervision was initiated with an inspection on 7 November 2019. In connection with IMY sending the inspection report to Bonnier News AB, IMY asked the company supplementary questions on 20 December 2019. Bonnier submitted its point of view on the inspection report and replied to IMY's questions on 14 February 2020. On 15 May 2020, IMY submitted further supplementary questions to Bonnier News AB, to which it replied on 11 June 2020. Due to Bonnier News AB's update of its personal data policy, the company submitted additional information on 21 July 2020.

Bonnier News AB has given its opinion on IMY's draft decision on 13 April 2023.

² DI-2018-22602, DI-2019-10121, DI-2019-10513, DI-2019-11057, DI-2019-7484, DI-2019-8104 and DI-2019-9556

As the case concerns cross-border processing, IMY has made use of the cooperation and consistency mechanisms provided for in Article 56 and Chapter VII of the GDPR. The concerned supervisory authorities have been the authorities of Denmark, Germany, Finland and Norway.

2.1 Description of the group common processing of personal data

The following circumstances have emerged during the inspection and subsequent exchange of documents. Within the Bonnier Group of companies there is a collaboration between Bonnier News AB and a number of affiliated companies that are part of the group of companies (the affiliated companies). Which companies are affiliated changes over time. At the time of the inspection, there were 15 affiliated companies, which decreased to 8 during the spring of 2020. The processing of personal data that takes place within the framework of the cooperation is limited to the affiliated companies customers on the Swedish market. The affiliated companies collect personal data from their customers and people who visit the company's websites. The data collected is transferred into two group common databases, one customer database (KDB) and one behavioural database (the behavioural database). These databases generate profiles of individuals. The profiles are also linked to information obtained from Bisnode Sverige AB.

Bonnier News AB has stated that it stores collected data in the group common databases in order to use for the following purposes:

- To establish a customer register for affiliated companies with good data quality, which includes compiling customer and user data and to verifying the accuracy, relevancy and appropriateness of the data
- To offer the customers of the affiliated companies an easy way to exercise their rights and an opportunity to ask questions about personal data to the joint customer service
- To make available personal data to affiliated companies in order to:
 - Use the contact details of other affiliated companies to enable marketing to the affiliated companies of its own products and services through postal direct marketing and telemarketing.
 - Display personalised content and ads in the affiliated companies digital services, based on customer and user's customer profile and behaviour on the affiliated companies sites.
 - Perform analysis of customer data to gain customer insight in order to conduct customer communications, marketing of its own products, services and customer service.
 - Perform analysis of customer data in order to improve and develop existing services and products.

The personal data processing that takes place for the purpose of adapting the advertisements of affiliated companies is based on data stored in the behavioural database. The personal data processing that takes place to disclose personal data to affiliated companies for use in telemarketing and postal direct marketing is based on data in KDB.

2.1.1 Description of the processing of personal data contained in the behavioural database

The inquiry in the case shows the following.

The data stored in the behavioural database is processed for the purpose of displaying personalised content and personalised advertisements in the digital services of the affiliated companies.

When an individual visits an affiliated company's website, the affiliated company collects information about the individual's browsing pattern. This is enabled through a script on the affiliated company's website requesting to save a text file (cookie) on the visitor's computer, tablet or mobile phone. The information contained in the cookie can be used to track the user's browsing pattern on the website. The data (behavioural data) collected when the individual browses and is then transferred to the behaviour database and added to the individual's profile is:

- Information on the URL (the visited webpage), its category and a content tag³.
- Information on the user's device in which the webpage view took place, the browser type and the part of the user's IP address identifying the country;
- Information on the behaviour in terms of the time spent on and time stamp for the page view;
- Information on a unique, randomly generated cookie value ('cookie identifier');
- Information on whether the page view took place in log-in mode.

Bonnier News AB erase the cookie identifier after 30 days and as of day 31, the generated behavioural data is no longer used for personalised advertisements to private individuals.

Data in the behavioural database and in KDB may in some cases be linked together.

Where the data in the behavioural database cannot be linked to KDB data, the behavioural profile of the data subject consists only of the data listed above, a profile which for the purposes of this decision will be referred to as "*simple behavioural profile*".

Where data in the behavioural database and data in KDB can be linked together in the behavioural database, data from KDB is added regarding the purchase history, gender, age, car ownership of the household and postal code, as well as statistical variables based on the private individual's residential area such as life phase, purchasing power and housing form to the behavioural database. For the purpose of this decision, these profiles will continue to be referred to as "*supplemented behavioural profile*".

The process of making data available to affiliated companies is done through a search tool that is linked to the behavioural database where the affiliated company can order a

³ A content tag is a description of the content that has been consumed in the services of the participating companies. Bonnier News AB collects two types of tags, predefined according to IAB's (The Interactive Advertising Bureau) standard and tags produced by the affiliated companies' editorial boards.

segment of customer data based on its chosen variables. An administrator will review whether the order meets the cooperation specific criteria. If this is the case, the affiliated company will gain access to a code that enables it to target ads at users included in the segment.

The affiliated companies can only retrieve data from the behavioural database based on behavioural data that has been collected from the company's own digital services. This applies regardless of whether it is a simple or supplementary behavioural profile. Regarding the supplemented behavioural profile however, it may contain purchase history from other affiliated companies as well. In KDB, data is erased after two years upon which data older than that cannot be linked to the behavioural database or disclosed to affiliated companies.

2.1.2 Description of the processing of personal data stored in KDB

The inquiry in the case shows the following.

The information about private individuals contained in KDB is processed for the purpose of being used by affiliated companies for the marketing of their own products and services through postal direct marketing and telemarketing.

In connection with an individual making a purchase or signing up to a subscription, the affiliated company that has a contractual relationship with the customer collects data from the customer. A portion of this data is transferred to KDB. In KDB, information is linked to a profile. In KDB, the customer profile is assigned a KDB ID. If the affiliated company's customer is already registered in KDB, the existing customer profile is updated/supplemented with the new engagement. In the absence of a pre-existing customer profile, a new customer profile is created with a new KDB ID. The data stored in KDB collected from the customer's contact with the affiliated company is the name, address, telephone number, national identification number national identification number, e-mail address and information related to the customer's purchase, such as product category, brand, type of packaging (whether it is a digital or traditional product and whether it is a free or paid product). It is also registered in the KDB if the customer has objected to its data in the KDB being used for marketing purposes and information whether the customer has registered in the so-called NIX register. There are limitations for the following categories of data:

- The e-mail address is not disclosed to affiliated companies for the purpose of telemarketing and postal direct marketing.
- The national identification number is only used to verify whether the customer has signed up to object to marketing measures in the NIX register (NIX-spärr) and to check that the customer is not deceased.
- The national identification number is not made available to the affiliated companies.

In addition to the data collected by the affiliated companies, Bonnier News AB collects data from Bisnode Sverige AB in order to control and supplement the contact details of individuals, as well as to provide statistical data such as life phase, purchasing power and form of housing. Furthermore, data on car ownership and deceased persons are collected as well as information on a so-called GEDI ID (which is a unique identifier in the form of a pseudonymized ID).

Data in KDB and the behavioural database may in some cases also be linked in KDB. The profile then constitutes what in this decision hereinafter will be referred to as *supplemented customer database profile*. This is done by a customer of an affiliated

company visiting the company's website and logging into his account. The behavioural data that has been collected regarding the customer and which is linked to a cookie identifier can under certain conditions be linked to the customer's KDB ID. In cases where the customer's KDB ID and the value of the cookie can be linked together, the KDB profile is supplemented with data collected in the last 30 days from the behavioural database. The data collected is information about which websites the customer has visited, which section of the website the customer visited (so-called content tags), and what device type the customer have used for browsing. Bonnier News AB has limited the type of content tags on which companies other than the one whose website the individual have accessed can base their profiling on for the purposes of telemarketing and postal direct marketing.⁴

When a person ceases to be a customer of an affiliated company, KDB is notified that the customer's engagement has ended and the customer is flagged as a passive customer. The customer's data will then be deleted in KDB after two years. Data collected from the behavioural database is deleted after 30 days. Any NIX blocking is always activated when making contact information in KDB available to other affiliated companies' customers and contact details of their own customers when they have been passive for 12 months.

The data is made available to affiliated companies upon request through an application in KDB. In KDB, a sample file is created based on the criteria specified by the affiliated company. Within the framework of the cooperation, something called purpose-adapted schemes is applied. These regulate what information is disclosed from KDB. At the point of disclosure, only the data points defined as necessary for the marketing channel indicated at the time of disclosure are provided, i.e. telephone numbers at a telemarketing campaign and addresses used for postal direct marketing. The data points on which the segmentation was based are not disclosed. The data is made available through an interface in KDB to the affiliated company.

It is possible for the data subject to request erasure from KDB. The data subject also has the right to object to the use of their data for telemarketing and postal direct marketing.

Bonnier News AB has stated that all affiliated companies are majority owned by Bonnier Group AB and are subject to the Bonnier Group's framework for processing personal data and that only a small part of the profiles in question could be linked to data in the behavioural database.

3. Statement of reasons for the decision

3.1 IMY's competence

3.1.1 Circumstances at issue

Part of the personal data processed within the group common cooperation has been collected through affiliated companies having placed a cookie on the visitor's computer, surf tablet or mobile phone. Bonnier News AB has stated that the collection is made through the websites of affiliated companies. The affiliated companies then transfer this data to the behavioural database and in some cases the data is also linked to profile information in KDB. Bonnier News AB has stated that the obligations arising from the provisions of the Electronic Communications Act (2003:389) and the

⁴ Only tags categorised with IAB's taxonomy are collected.

since adopted Electronic Communications Act (2022:482) on Electronic Communications (LEK), aimed at affiliated companies and not Bonnier News AB because it is the affiliated companies that are responsible for the processing that is the actual collection of the data.

3.1.2 Applicable provisions, etc.

Pursuant to Article 95 of the GDPR, the GDPR shall not impose any additional obligations on natural or legal persons that process personal data within fields that are already subject to obligations under the so-called ePrivacy directive⁵. The ePrivacy directive has been implemented in Swedish law through LEK, where, *inter alia*, the collection of data through cookies is regulated.

Pursuant to Chapter 9, Section 28 of the LEK, data may be stored in or gained from a subscriber's or user's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and has given his consent to it. Furthermore, it follows that this does not prevent the storage or access necessary to transmit an electronic message over an electronic communications network or which is necessary for the provision of a service expressly requested by the user or subscriber. Prior to August 1st 2022, when the LEK entered into force, corresponding requirements were made pursuant to Chapter 6, Section 18 of the Electronic Communications Act (2003:389). The Swedish Post and Telecom Agency (PTS) is the supervisory authority pursuant to the LEK (Chapter 1, Section 5 of Ordinance [2022:511] on electronic communications).

The EDPB has stated in its opinion on the interplay between the ePrivacy directive and the General Data Protection Regulation⁶. It follows, *inter alia*, that the national supervisory authority appointed under the ePrivacy directive is solely competent to oversee compliance with the directive. However, according to the GDPR, the supervisory authority is the competent supervisory authority for the processing which is not specifically regulated in the ePrivacy directive. If only part of the processing falls within the scope of the ePrivacy directive, this does not limit the supervisory authority's power to examine other parts of the processing pursuant to the GDPR.⁷

This means, *inter alia*, that the data protection authority under the GDPR is competent under the GDPR to assess the lawfulness of the processing of personal data that takes place after the data has been retrieved from the individual's terminal equipment, such as the storage of collected data and the analysis of data for purposes of online behavioural advertising.⁸

3.1.3 IMY assessment

The data supplied to the behavioural database has been collected by the affiliated companies through cookies. The processing of personal data that is under investigation in this supervisory case is Bonnier News AB's subsequent processing of personal data in the behavioural database. Said processing is not covered by the regulations in the LEK or the previously applicable regulation in the Electronic

⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

⁶ Opinion 5/2019 on the interaction between the ePrivacy Directive and the general public General Data Protection Regulation, in particular as regards the competences, tasks and powers of data protection authorities, adopted on 12 March 2019

⁷ See paragraphs 68 and 69 of the opinion.

⁸ See paragraph 75 of the opinion.

Communications Act (2003:389). This means that the GDPR applies to the processing and that IMY is the competent supervisory authority.

3.2 Bonnier News AB's responsibility for the data processing

3.2.1 Circumstances at issue and Bonnier News AB's position

It is Bonnier News AB's position that Bonnier News AB and each affiliated company have a joint controllership and responsibility for the processing that takes place in KDB and the behavioural database for the purposes set out above as common.

Furthermore, Bonnier News AB has stated that Bonnier News AB and its affiliated companies share a joint view of the purposes and means and that Bonnier News AB has entered into the Joint Data Controller Agreement with the affiliated companies pursuant to Article 26(2) of the GDPR.

Bonnier News AB has stated that each affiliated company has its own independent ("local") controller responsibility for its own collection of the data. Bonnier News AB has further stated that it has no joint controller responsibility for the personal data processing carried out at the point after which the data has been disclosed to affiliated companies from the group common databases. It is the affiliated company that retrieves the data that is responsible for the processing carried out by this company after collection.

3.2.2 Applicable provisions, etc.

Pursuant to Article 4(7) of the GDPR, the controller is the person who alone or jointly with others determines the purposes and means of the processing of personal data. The fact that the purpose and means can be determined by more than one actor means that several actors can be controllers for the same processing.

Pursuant to Article 4(2) of the GDPR, processing is a measure or combination of measures involving personal data or sets of personal data.

The Court of Justice of the European Union has held in the Fashion-ID judgement that a website owner who uses social network plug-ins on its website may become a joint controller with the social network. This applies to the processing of collection and disclosure by transmission of the personal data of website visitors using the social network plug-in. The Court also held that each party is responsible only for those parts of the processing chain for which it actually determined the purpose and means.⁹

In Wirtschaftsakademie, the Court of Justice held that joint controller responsibility for processing does not necessarily mean that the various actors involved in the processing of personal data have the same responsibility.¹⁰ On the contrary, those actors may be involved at different stages of the processing of personal data and to different degrees, for which each actor's level of responsibility must be assessed in the light of all the relevant circumstances of the individual case.

3.2.3 IMY assessment

Bonnier News AB provides two databases, the KDB and the behavioural database, from which data from affiliated companies are merged into profiles of private individuals. Subject to the conditions determined by Bonnier News AB and the

⁹ See judgment in Fashion-ID, C-40/17, EU:C:2019:629, paragraph 64-85

¹⁰ See judgment in Wirtschaftsakademie, C-210/16, EU:C:2018:388, paragraph 43

companies, the information is made available to Bonnier News AB and affiliated companies.

IMY notes that, in addition to making the databases available to the affiliated companies, Bonnier News AB has together with the companies decided the framework for the processing in various ways.

In light thereof, IMY makes the assessment that Bonnier News AB is joint controller of the data along with the affiliated companies for the part of the personal data processing that takes place for the common purposes of making personal data available, through profiling of private individuals' data, to affiliated companies to display personalised advertisements and for use in telemarketing and postal direct marketing. This includes the collection of data to the databases, the storage in the databases and the profiling, the collection of additional data from Bisnode Sverige AB, the interconnection that occurs between the behavioural database and KDB, and the transfer of data between the databases. Furthermore, Bonnier News AB is jointly responsible for personal data with the affiliated companies for the actions that take place before and upon a disclosure to an affiliated company.

3.3 What constitutes personal data?

3.3.1 Circumstances at issue and Bonnier News AB's position

Under the section titled "Description of the group common personal data processing" the processing is described as a variety of data collected from private individuals are processed in KDB and the common behavioural database. Bonnier News AB considers that what is referred to in this decision as supplemented behavioural profile constitutes personal data. However data in the behavioural database – which cannot be linked to data in KDB – constitute anonymous behavioural data according to Bonnier News AB. This is because they cannot be linked to a person either via KDB ID, customer ID, IP address or any other identifier of a person. Bonnier News AB therefore considers that the behavioural profiles referred to in this decision as simple behavioural profiles do not constitute personal data. The segmentation made on these simple profiles is, according to Bonnier News AB, only based on the affiliate's own collected information in the behavioural database (a company can, for example, choose to adapt sports-related content and advertisements to the data recorded via a cookie in the last 30 days).

3.3.2 Applicable legal provisions other legal sources

Pursuant to Article 4(1) GDPR, personal data is any information relating to an identified or identifiable natural person (i.e. the data subject). From the same provision, it follows that an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or online identifiers or one or more factors specific to the natural person's physical, physiological, genetic, mental, economic, cultural or social identity.

According to Recital 26 of the GDPR, the principles of data protection should apply to all information relating to an identified or identifiable natural person. Personal data which have undergone pseudonymisation which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all means, such as singling out which, either by the controller or by another person, may reasonably be used to identify the natural person directly or indirectly. In order to determine whether means are reasonably likely

to be used to identify the natural person, account should be taken of all objective factors, such as the costs and duration of identification, taking into account both the available technology at the time of processing and technological developments. The principles of data protection according to recital 26 should not apply to anonymous information that does not relate to an identified or identifiable natural person, or to personal data rendered anonymized in such a way that the data subject is no longer identifiable. The Regulation therefore does not concern the processing of such anonymous information, which includes information for statistical or research purposes.

According to recital 30 of the GDPR, natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses, cookie identifiers or other identifiers, such as radio frequency identifications tags. This may leave traces that, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of natural persons and identify them.

An opinion of the Article 29 Working Party,¹¹ which contains an analysis of the concept of personal data, shows that a natural person in a group is considered to be 'identified' when he or she can somehow be 'singled out' from other persons.¹² The European Data Protection Board (EDPB) has stated in its guidelines on targeting users through social media advertising that even persons who use a social media service without having created an account or profile with the social media service may constitute data subjects within the meaning of Article 4(1) of the GDPR if the person is directly or indirectly identified or identifiable.¹³ In that regard, the EDPB refers to the concept of 'singling out' in recital 26 of the GDPR and to the abovementioned opinion of the Article 29 Working Party.

The Article 29 Working Party's opinion on online behavioural based advertising further develops what it means to be identifiable:

The Article 29 Working Party states that behavioural based advertising often leads to the processing of personal data. Behavioural based advertising typically includes the collection of IP addresses and the processing of unique identifiers (through the web cookie). The use of such functions with a unique identifier makes it possible to track users of a particular computer even if dynamic IP addresses are used. In other words, such functions make it possible to "singled out" individual data subjects, even if their names are not known. In addition, the information collected in behavioural advertising relates to (i.e. is about) a person's characteristics or behaviour and is used to influence that particular person. This approach is further reinforced by taking into account the possibility that profiles can be linked at any time to directly identifiable information provided by the data subject, such as information provided when registering on a website. Other scenarios that may lead to identification include mergers, data losses and the growing availability of personal data linked to IP addresses on the Internet¹⁴

¹¹ The so-called Article 29 Working Party was an advisory and independent working group composed of representatives of the supervisory authorities of the EU and the EEA. The task of the group was to contribute, inter alia, to the uniform application of the Data Protection Directive through recommendations. The Working Party has been replaced on 25 May 2018 by the EDPB.

¹² See WP 136. Article 29 Working Party Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, p 12(f)

¹³ See EDPB Guidelines 8/2020 on Targeted Advertising in Social Media Version 2.0, adopted 13 April 2021, p 19

¹⁴ See WP 171, Opinion 2/2010 of the Article 29 Working Party on behavioural advertising on the Internet, adopted on 22 June 2010, p. 9(f)

3.3.3 IMY's position

IMY notes that the supplemented behavioural profiles (i.e. behavioural profiles linked to KDB) contain data relating to identified or identifiable natural persons. The supplementary behavioural profiles are therefore personal data.

With regard to the simple behavioural profiles (i.e. behavioural profiles not linked to KDB), IMY makes the following assessment.

In order for a data to be classified as personal data, it is necessary, first, that the data refers to a natural person. This requirement is met with regard to simple behavioural profiles because the data describe how the individual has surfed with a number of different parameters.

Furthermore, the natural person is required to be identified or identifiable. According to Article 4(1) of the GDPR, it is sufficient for a person to be identified indirectly for this requirement to be met. The provision further states that identification may be made by reference to an online identifier. Recital 30 of the Regulation lists cookies ("cookie identifiers" in the English language version) as an example of online identifiers. Identification within the meaning of Article 4(1) may therefore be carried out by means of unique web cookie values used in the behavioural database.

IMY further notes that from recital 26 of the GDPR it becomes apparent that singling out is a means of identifying a natural person. This means that one person can be identified by being distinguished from other persons.¹⁵ Thus, it is not required that the person be identified by name or national identification number. Such separation or screening occurs when the information being processed makes it possible to identify, draw conclusions or take specific action in relation to a user. In the behavioural database, the information is linked to a unique identifier, a unique cookie value, which is linked to a specific browser or app, which in turn is connected to a device such as a computer or phone. One of the purposes of the processing of the data is to target users through marketing based on the users previous behaviour in an identified browser or app on the basis of the user's behaviour. The purpose of the processing is thus to draw conclusions about the individual by creating a profile and based on this affect the individual. Thus, IMY notes that even the simple behavioural profiles not linked to KDB mean that individuals are identifiable.

Against this background, IMY considers that the simple behavioural profiles constitute personal data.

3.4 The processing constitutes profiling

3.4.1 Applicable provisions

Profiling is defined in Article 4(4) of the GDPR as any form of automated processing of personal data that consists of the use of personal data to assess certain personal characteristics of a natural person, in particular to analyse or predict that natural person's performance at work, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.

¹⁵ See WP 136.f Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007 p. 12

3.4.2 IMY's position

IMY notes that the processing, both of personal data based on simple behavioural profiles and supplemented behavioural profiles that take place for the purpose of making the data available to affiliated companies for the purpose of displaying personalised advertisements includes profiling of data subjects as defined in Article 4(4) of the GDPR. This is because it concerns the automatic processing of personal data aimed at categorising the data subjects according to their previous behavioural patterns, which in turn makes it possible to assess some of their personal characteristics.

IMY further notes that the processing of personal data for the purpose of making available contact details for telemarketing and postal direct marketing includes profiling of data subjects as defined in Article 4(4) of the GDPR. This is because it involves automated processing of personal data for the purpose of categorising data subjects based on their purchase history and, in some cases, also behavioural patterns.

3.5 Legal basis for processing for the purpose of displaying personalised advertisements based on data in the behavioral database

3.5.1 Circumstances at issue and Bonnier News AB's position

Bonnier News AB has stated that the activities within the Group has been coordinated in order to achieve a better data collection and make it possible to process the customers' and users' personal data for specified purposes in a cost-effective and integrity-friendly manner. Bonnier News AB uses profiling of private individuals to make data available to its affiliated companies for the purpose of displaying personalised advertisements, on collected behavioural data that cannot be linked to KDB, and on behavioural data which can be connected to the KDB and where additional personal data is added to the data subject's profile. Bonnier News AB relies on the legal basis of Article 6(1)(f) of the GDPR for this processing of personal data.

Legitimate interest

Bonnier News AB has stated the following.

The Company has a legitimate interest which consists in a need to understand its customers and users wishes and needs in order to achieve relevance in content and advertising targeted at customers and users and through it be able to offer competitive products/services and attractive advertising spaces. Many of the affiliated companies also engage in journalistic operations. Today, publishers' business model consists of revenue streams from reader and advertising income. The group common personal data processing is important for the financing of the companies' journalistic operations. Bonnier News AB has also pointed out the protection of freedom and diversity of the media in Article 11 of the EU Charter of Fundamental Rights.

Necessary processing

Bonnier News AB has stated that the processing of personal data is necessary in order to achieve the purposes of making available private individuals' profiles to affiliated companies in order to display personalised advertisements. The company, along with the other companies, has taken steps to minimise the number of data collected as well as to limit the duration of the processing of the data and to ensure that the databases are kept separate and that only certain data are transferred between them.

Balancing of interests

Bonnier News AB has stated the following.

Bonnier News AB's interest overrides the private individual's interest in the protection of their personal data.

The processing of personal data in order to display personalised advertisements based on the private individual's profile is an essential condition for journalists and publishers to earn revenue and by extension be able to conduct journalism.

There is a possibility to object to the profiling that is based on behavioral data. According to the information that private individuals receive in Bonnier News AB's personal data policy, the private individual can object to information about their online behaviour being processed in the group common customer database.¹⁶ The result is that the connection between the private individual's customer data and their browsing behaviour is removed.

The data subjects have a direct relationship with one or more affiliated companies. Users/customers have either visited an affiliated company's website, purchased products from an affiliated company or have an active digital subscription. Many of the customers are subscribers who have a long-term relationship with the company providing the service or product and can therefore be considered to reasonably expect that their data will be processed. Many readers have a strong commitment to their preferred type of news media. Customer profiles in KDB contains, to some extent, to unit-purchases such as literature, newspaper and goods. In these cases, the relationship between customer and supplier may be considered somewhat less unique. Furthermore, the interaction is voluntary, clear information is provided and there are alternative products such as printed newspapers that private individuals can view completely anonymously.

It is unlikely that the processing will have a negative impact on the data subject's interest. Private individuals' interaction with affiliated companies is voluntary and it is in their interest that the companies' services are as relevant as possible. Furthermore, Bonnier News AB has referred to the fact that the Article 29 working party has stated that targeted marketing based on simple customer profiles, such as gender, age, place of residence and general interests (e.g. "fashion") typically has no significant impact on private individuals. Furthermore, Bonnier News AB has taken steps to ensure that a minimum of data is processed in relation to the purposes as well as to reduce privacy risks in other respects. Among other things, the personal data is not shared with companies other than the affiliated companies within the group and all of these companies are subject to the Bonnier Group's framework for processing of personal data.¹⁷

The processing at issue falls within the data subject's reasonable expectations because the private individuals who come into contact with the companies do so out of their own free will in order to access content on websites, purchase services and/or products and that they always have a customer/user relationship with one or more companies within the group. The companies' privacy policies contain easy to understand information about how the processing of customers' and users' personal

¹⁶ The version of Bonnier News AB's personal data policy filed on 21 July 2020, see under the heading "How to access and control your personal data", file annex 20.1.

¹⁷ Further measures taken are set out in the opinion submitted on 14 February 2020 Annex 13, Annex O

data is conducted within the group. The processing carried out within the scope of the KDB and the behavioural database is closely related to the companies' services and products, which should indicate what the consumers can expect. The fact that many of the companies' products and services are provided online and, in many cases, free or funded through advertising should lead to a certain expectation and acceptance of certain personal data processing for, inter alia, the adaptation of content and advertising. Today, many digital products that are consumed by a very large proportion of consumers in society are adapted to the individual and it is Bonnier News AB's point of view that today's consumers expect that the digital products and services they consume to some extent will be adapted to the private individual.

3.5.2 Applicable provisions, etc.

Personal data shall be processed in a lawful, fair and transparent manner in relation to the data subject, pursuant to Article 5(1)(a) GDPR. The lawful processing of the data means, inter alia, that at minimum one of the conditions set out in Article 6(1) is fulfilled.

Consent pursuant to Article 6(1)(a), is one of the legal bases a controller can rely upon for the processing of personal data. Another legal basis pursuant to Article 6(1)(f) is legitimate interest, which requires that the following three cumulative conditions are met. There must be (i) a legitimate interest of the controller or of the third party to whom the data is disclosed, (ii) the processing of personal data must be necessary for the legitimate interest pursued by the controller and (iii) the data subject's interest in the protection of his or her personal data must not outweigh the interest of the controller.¹⁸

According to recital 47 of the GDPR, a legitimate interest may exist, for instance, where there is a relevant and appropriate relationship between the data subject and the controller, for example if the data subject is a customer of the controller. It is stated that the processing of personal data for direct marketing purposes may be regarded as a legitimate interest. Furthermore, it is stated that a legitimate interest requires a careful pre-assessment, including if the data subject can reasonably expect, at the time and in connection with the collection of personal data, that processing for the specified purpose may take place. The interests and fundamental rights of the data subject could, in particular, triumph that of the controller if personal data are processed in circumstances where the data subject cannot reasonably expect any further processing.

Pursuant to Chapter 9, Section 28 of the LEK, which implements Article 5(3) of the ePrivacy Directive in Swedish law, data may be stored in or retrieved from the user's or subscriber's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and consents to it. This does not prevent the storage or access necessary to transmit an electronic message over an electronic communications network or that is necessary to provide a service explicitly requested by the user or subscriber. Similar requirements previously applied in accordance with Chapter 6, Section 18 of the Electronic Communications Act (2003:389).

The EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications show that data collected on the basis of consent pursuant to Article 5(3) of the ePrivacy Directive or subject to the exceptions

¹⁸ See, Fashion ID, C-40/17, EU:C:2019:629, paragraph. 95.

in Article 5(3) of that Directive can only be further processed for another purpose, if the controller requests further consent or is supported by Union or Member State law.¹⁹ The EDPB further states that such further processing cannot be based on a compatibility test pursuant to Article 6(4) GDPR, as it would undermine the protection of the ePrivacy Directive. Furthermore, the EDPB states that consent must, when required by the ePrivacy Directive, be specific and informed, meaning that data subjects must be made aware of each one of the purposes for processing and have the right to refuse such specific purposes. Should further processing on the basis of a compatibility test under Article 6(4) GDPR be possible, the very principle of consent requirements of the current Directive would be circumvented²⁰

In the EDPB Guidelines on the targeting of social media users, personal data are divided into categories of data that the data subject actively and knowingly has provided to the controller, observed data provided by the data subject through his or her use of the service or entity and derived and inferred data created on the basis of the data provided by the data subject.²¹ According to the EDPB, there are two lawful bases that could be considered for processing such data that the data subject has actively and knowingly provided, those being consent under 6.1(a) and legitimate interest under 6.1 f GDPR. Regarding data collected through observed data provided by the data subject through the use of a service or entity, including data collected through cookies, the EDPB states that Article 6(1)(f) cannot provide a lawful basis for targeted advertising where private individuals are tracked across websites and locations.²² Furthermore, the EDPB states that for such processing, consent is probably the most appropriate lawful basis in Article 6 GDPR. The assessment should also consider the fact that the processing includes activities that the EU legislator has opted to provide additional protective measures.²³

In its guidelines on consent under Regulation 2016/679, the EDPB has stated that if controllers choose to rely on consent as lawful basis for any part of the processing, they must be prepared to respect this choice and stop this part of the processing if a private individual withdraws their consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals. In other words, the controller cannot swap from consent to other lawful bases. The EDPB further states that, for instance, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.²⁴

According to an opinion of the Article 29 Working Party on the notion of the controller's legitimate interest in Directive 95/46/EC, when carrying out the balancing of interests test, account should be taken of the nature of the controller's legitimate interest, the damage to the controller if the data were to not be processed, the nature of the data, the way data are being processed, the status of the data controller and data subjects., the reasonable expectations of the data subjects as to what will happen to

¹⁹ See Guidelines 01/2020 on the processing of personal data in connection with connected vehicles and mobility-related applications, Version 2.0, Adopted on 9 March 2021, para. 53

²⁰ See previous note

²¹ See EDPB Guidelines 8/2020 on Targeted Advertising in Social Media Version 2.0, adopted 13 April 2021, para. 40

²² See previous note, paragraph 77

²³ See previous note paragraph 78

²⁴ See EDPB Guidelines 05/2020 on consent under Regulation (EU) 2016/679, Version 1.1, adopted on 4 May 2020, paras 122-123

their data and the consequences for the data subjects. If, after analyzing the above factors, the outcome of the balancing of interests' test is still unclear, the design of so-called additional safeguards may be decisive for the outcome of the balancing of interests' test.²⁵

The Article 29 Working Party guidelines on automated individual decision-making and profiling, provide guidance when profiling can be based on legitimate interests under 6.1(f). According to the Guidelines, the following elements are relevant:

- The level of detail in the profile.
- The comprehensiveness of the profile.
- The impact of the profiling.
- The safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.

In several opinions, the Article 29 Working Party has repeated its position that it is difficult to rely on Article 6(1)(f) GDPR for profiling that takes place for marketing or advertising purposes when private individuals are tracked across multiple websites, locations, entities, services or for data brokerage activities.²⁶

3.5.3 Basic principles for IMY's assessment

Bonnier News AB processes personal data for the purpose of making individuals' profiles available to affiliated companies in order to display personalised advertisements based on the lawful basis legitimate interest pursuant to Article 6(1)(f) of the GDPR. Before IMY examines whether the lawful basis may constitute the basis for Bonnier News AB's processing, IMY finds reason to consider how the processing relates to certain statements made in the EDPB guidelines.

According to the EDPB's guidelines on the targeting of social media users, regarding data that the data subject has actively and knowingly provided, both consent and legitimate interest may constitute a lawful basis for the processing. However, the guidelines show that for data collected through observation (e.g. through cookies), legitimate interest cannot serve as an appropriate lawful basis when targeted advertising is based on tracking individuals across websites and locations.

IMY points out that Bonnier News AB collects data for its behavioral database from several different websites, but an affiliated company can only retrieve data based on behavioural data collected from the company's own digital services. This applies regardless of whether it is a simple or supplementary behavioral profile.

The EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications state that data collected on the basis of consent pursuant to 5.3 of the ePrivacy Directive can be further processed for another purpose only if the controller requests further consent or the processing is supported by EU or national law. The EDPB guidelines on consent in its section on interplay between consent and other lawful bases in Article 6 also addresses the situation when

²⁵ See Article 29 Working Party Opinion 6/2014 on the notion of the controller's legitimate interests in Article 7 of Directive 95/46/EC

²⁶ See the Opinion of the Article 29 Working Party on Automated Individual Decision-Making and Profiling under Regulation (EU) 2016/679, adopted on 3 October 2017, p. 15 and Opinion 6/2014 of the Article 29 Working Party on the concept of the controller's legitimate interest in Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 47, and the examples of pp. 59-60 and EDPB Guidelines 8/2020 on targeted advertising in social media Version 2.0, adopted on 13 April 2021 p. 77

the data subject is informed that data will be processed on the basis of consent, while actually some other lawful basis is relied on, is fundamentally unfair to individuals.

IMY notes that the situation in the supervisory case differs to some extent from that described in these guidelines. In the supervisory case, it is the affiliated companies that collect the data in pursuant to 5.3 of the ePrivacy Directive and are therefore subject to the requirement of consent in said provision. The affiliated companies have to ensure that they have legal support for their processing under the ePrivacy Directive and the General Data Protection Regulation. The processing of personal data by the affiliated companies is not covered by this supervision.

It is not Bonnier News AB that collects the data on the basis of consent under the national provisions implementing Article 5(3) of the ePrivacy Directive. It is only when the affiliated companies enter the personal data into the behavioral database and KDB that Bonnier News AB's processing begins. Bonnier News AB therefore does not change lawful basis from consent to legitimate interest.

At the same time, IMY points out that Bonnier News AB is part of the same Group of companies as the affiliated companies and that Bonnier News AB is a joint controller with the affiliated companies for the processing of personal data in the databases. The establishment of group common databases should not mean that data subjects receive a lower level of protection than if the processing took place only at the group company that collected the personal data. In other words, Bonnier News AB should not have greater opportunities to process personal data on the lawful basis of legitimate interest than that of the affiliated companies. Therefore, according to IMY, the guidelines set out above should have an impact on the assessment of the possibility of using legitimate interest as a lawful basis in the supervisory case.

It can be inferred from the above stated that, pursuant to Article 6(1)(f) of the GDPR, the scope for further processing of data collected on the basis of consent under the LEK is very limited. At the same time, the GDPR does not prohibit the use of Article 6(1)(f) as the lawful basis for the type of processing in question. IMY therefore proceeds and examines whether the processing is based on Article 6(1)(f) of the GDPR. IMY's assessment of whether Bonnier News AB can rely its processing on Article 6(1)(f) of the GDPR is based on the three conditions that must be fulfilled under the provision:

- (i) Is there a legitimate interest of the controller or of the third party to whom the data are disclosed?
- (ii) Is the processing of personal data necessary for the legitimate interest pursued?
- (iii) Does the data subject's interest in protecting his or her personal data outweigh the controllers?

IMY deals with the first two steps of the balancing of interests test jointly for the supplemented and simple behavioural profiles (sections 3.5.3 and 3.5.4). The third and final steps are then dealt with separately for the supplemented behavioural profiles (section 3.5.5) and the simple behavioural profiles (section 3.5.6).

3.5.4 Legitimate interest

There is a commercial aspect to Bonnier News AB's interest in creating profiles to make data available to affiliated companies in order to display personalised ads. The commercial aspect of an interest does not preclude that the interest is justified, but determines whether that interest is lawful, specific and represent a real and present interest.²⁷

Bonnier News AB's and affiliated companies' interest is lawful, real and present. IMY therefore notes that Bonnier News AB's interest in creating profiles for making available as well as the affiliates' interest in processing personal data in order to display personalised advertisements based on customer and user customer profiles and behavioural profiles is legitimate.

3.5.5 Is the processing necessary for the legitimate interest?

The necessity requirement laid down in Article 6(1)(f) of the GDPR must be examined in conjunction with the principle of data minimisation set out in Article 5(1)(c).²⁸ The purpose of the processing is to make data available to affiliated companies in order to display personalised advertisements based on private individual profiles. The supervisory case has shown that Bonnier News AB, together with the affiliated companies, has taken steps to minimise the number of data collected and limit how long this data is processed, as well as to ensure that the databases in which the data are processed are kept separate and that only certain data are transferred in between the two databases. In light thereof, IMY considers that the processing described in this Decision is necessary for the stated purpose.

3.5.6 Balancing test for the processing of personal data in supplemented behavioural profiles

Bonnier News AB's interest in creating profiles to make data available to affiliated companies in order to display personalised advertisements can, according to the company, benefit the private individual either through higher revenues allowing for free or cheaper services or that the individual is provided with offers that they are interested in. Bonnier News AB has also emphasised that many of the affiliated companies are engaged in journalistic operations and that publishers' operating model of today consists of income streams from reader and advertising revenue and that the group common processing is important for the financing of the companies' journalistic operations. In those circumstances, the company considers that its interest is particularly important.

As IMY has already stated, the interest in displaying personalised advertisements is justified pursuant to and within the meaning of Article 6(1)(f) GDPR. On the question of the significance of this interest, IMY points out that the interest is not in itself journalistic, but of a commercial nature. Through profiling, knowledge about customers and potential customers is achieved, which enable revenue from personalised advertising. IMY considers that Bonnier News AB's and its affiliated companies' commercial interest does not weigh as heavily as Bonnier News AB claims.

As regards the assessment of the interests of data subjects, IMY considers the following.

²⁷ See Article 29 Working Party Opinion 6/2014 on the notion of the controller's legitimate interests in Article 7 of Directive 95/46/EC

²⁸ See judgment in Asociația de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064, paragraph 48

As pointed out above, Bonnier News AB collects personal data in the behavioural database that was originally collected by the affiliated companies through cookies. The consent requirement under Chapter 9, Section 28 of the LEK for the collection provides a high level of privacy protection and a possibility for data subjects to control the use of the collected data.²⁹ This protection, as stated by the EDPB in several of its guidelines, risks being undermined if the personal data collected are processed on the basis of other lawful bases, such as legitimate interest pursuant to Article 6(1)(f) GDPR. As IMY already has stated, Bonnier News AB should not have more possibilities than the affiliated companies to use the lawful basis, legitimate interest, for processing the personal data, than the affiliated companies which collect them by cookies. IMY therefore considers that the nature of the data implies that the interest of the data subjects should be given great weight in the balancing of interests test.

Furthermore, IMY considers that the possibility for using Article 6(1)(f) GDPR as the lawful basis for profiling based on observed data is limited (see EDPB Guidelines 8/2020 on targeted social media advertising p. 77-78). IMY notes that the nature of the processing also means that the privacy interest of the data subjects weighs heavily.

Bonnier News AB has pointed out that profiling and personalised advertisements can benefit the data subject by enabling higher revenues for the affiliated companies, which in turn enables them to offer free or cheaper services. It can also benefit the data subject by providing them with offers that they are interested in. IMY does not question that the processing may partly benefit the data subjects, but believes that the overall interest in profiling is to create advertising that is as accurate as possible in order to get customers and potential customers to buy goods or services and to receive revenue from such advertising.

In cases where behavioral data can be linked to KDB for the purpose of displaying personalised ads (the so-called “supplementary behavioral profiles”), IMY considers the following in its assessment. While data for profiling are not collected from different websites, which, according to the EDPB guidelines, would render the lawful basis in Article 6(1)(f) GDPR as appropriate, the profiling includes data collected from other contexts such as previous purchases, collected demographic data and statistical data. IMY considers that profiling is extensive in its nature and that such profiling is not something a data subject can expect without having consented to such processing of personal data.

In conclusion, IMY considers that the data subject's privacy interest outweighs the interests of Bonnier News AB and its affiliated companies.

In light thereof, IMY concludes that Bonnier News AB has processed personal data in breach of Article 6(1) GDPR in order to profile the data subjects based on their behavioural data in a so-called supplemented behavioural profile and make the profiles available to affiliated companies in order to display personalised advertisements.

3.5.7 Balance of interests for the processing of personal data in simple behavioural profiles

As IMY previously stated in section 3.5.5, Bonnier News AB's interest to create profiles to make data available to affiliated companies to show personalised ads is a commercial interest that does not weigh as heavily as Bonnier News AB claims.

²⁹ The same requirements under Chapter 6, Section 18 of the Electronic Communications Act (2003:389) applied at the time in the case.

Regarding the assessment of the interests of data subjects, IMY takes into account the following.

Bonnier News AB has taken measures to minimise the number of data collected, implemented privacy-enhancing rules in segmentation, introduced rules of deletion and ensured that data collected from an affiliated company can only be used by that company. Thus, profiling takes place only on a company's "own visitors".

Furthermore, Bonnier News AB, through its integrity policy, informs about the processing.

What has been stated above must be weighted against the fact that the collection and profiling of simple behavioural profiles allows for the mapping of individuals through observed data that entails a greater infringement of privacy than when the data were collected through the involvement of the data subject. IMY considers that the privacy interest of data subjects is of great significance due to the nature of the data (the fact that special protection in LEK is given to the collection of the data). As IMY has already stated, Bonnier News AB should not have greater possibility than the affiliated companies to base their processing on legitimate interest than the affiliated companies which collected the personal data using cookies. Furthermore, IMY believes that when private individuals surfing behaviour is monitored to display personalised advertising, this can give the data subject the feeling of loss of control over their data and the feeling of being monitored. This may result in private individuals being affected in the choice of what they see on a website.

In conclusion, IMY considers because the processing enables profiling of individuals, that the data subject's privacy interest outweighs the interests of Bonnier News AB and affiliated companies when processing personal data in simple behavioural profiles

In light thereof, IMY notes that Bonnier News AB has processed personal data without having a lawful basis pursuant to Article 6(1) GDPR in order to profile the data subjects based on their behavioural data in so-called simple behavioural profiles and make the profiles available to affiliated companies for the purpose of displaying personalised advertisements.

3.6 Legal basis for processing for the purpose of making contact information available for telemarketing and postal direct marketing

3.6.1 Applicable provisions, etc.

In order to be able to rely on Article 6(1)(f) GDPR, as explained above, the three conditions set out in the article must be fulfilled. There must be a legitimate interest of the controller or of the third party to whom the data are disclosed, the processing of personal data must be necessary for the legitimate interest pursued and the interest of the data subject in the protection of his or her personal data must not prevail that of the controller.³⁰

The Guidelines of the Article 29 Working Party and the EDPB on profiling and the application of Article 6 have been set out in Section 3.5.

³⁰ Judgment of the Court of Justice of the European Union Fashion ID, C-40/17, EU:C:2019:629, para. 95.

3.6.2 Circumstances at issue and Bonnier News AB's position

Bonnier News AB has stated that it has coordinated its activities in order to achieve a better data base and enable the personal data of customers and users to be processed for specified purposes in a cost-effective and privacy-friendly manner. Bonnier News AB creates profiles on individuals in order to make contact information available for telemarketing and postal direct marketing. The profiling that this entails is partly based on data in KDB collected from affiliated companies during purchases and subscriptions (so-called customer engagements), and partly on data collected from Bisnode Sverige AB and, for a small part of the profiles, data from the behavioural database. Bonnier News AB relies its processing on Article 6(1)(f) GDPR.

Legitimate interest

Bonnier News AB has stated that the affiliated companies have a legitimate interest in marketing their products and services in an efficient and privacy-friendly way.

Necessary treatment

Bonnier News AB has stated that they together with the affiliated companies have taken steps to minimise the number of data collected, how long data is being processed and, in order to comply with the data minimisation principle, kept the databases separated and only transferred certain data. Furthermore, Bonnier News AB has taken steps to ensure that no more information than is needed is disclosed to the affiliated companies. At the time of disclosure, only the data points defined as necessary for the marketing channel indicated at the time of disclosure are provided, i.e. telephone numbers in a telemarketing campaigns and postal direct marketing address. The data points on which segmentation was based are not disclosed.

Balancing of interests test

Bonnier News AB has stated the following.

Bonnier News AB's interest in making data available to affiliated companies based on the data subject's profile for the purpose of telemarketing and postal direct marketing outweighs the data subject's privacy interest.

By using the Group's existing resources for telemarketing and postal direct marketing, rather than buying the same information/resource from an external party, a cost saving is generated while allowing for a more controlled utilisation rate of addresses and phone numbers than would have been possible otherwise. The processing is also intended to save purchase costs.

Bonnier News AB, together with the affiliated companies, has taken steps to minimise the number of data collected, limit how long data is processed and in order to comply with the data minimisation principle, keep the databases separate. For the purposes of telemarketing and postal direct marketing, Bonnier News AB has limited the type of content tags generated by the data subject browsing on other companies' websites.³¹ Furthermore, a link between the databases could only be made with a small percentage of users.

³¹ Only tags categorised with IAB's taxonomy are collected.

Furthermore, within the framework of the cooperation, what is known as purpose-adapted schemes is applied. These regulate what information is disclosed from KDB. At the time of disclosure, only the data points defined as necessary for the marketing channel indicated at the time of disclosure are provided, such as telephone numbers in a telephone sales campaign and postal direct marketing address. The data points on which segmentation was based are not disclosed.

There is a possibility for the data subject to request deletion from the group common database. The data subject also has the right to object to the data being used for telemarketing and postal direct marketing.

The data subjects have a direct relationship with one or more affiliated companies. Users/customers have either visited an affiliated company's website, purchased products from an affiliated company or have an active digital subscription. Many of the customers are subscribers who have a long-term relationship with the company providing the service or product, and can therefore be considered to have a greater expectation that their data will be processed. Many readers have a strong commitment to their preferred type of news media. To some extent, customer profiles in KDB belong to unit-purchases such as literature, newspaper and goods purchases, where the relationship between customer and supplier may be considered somewhat less unique. Furthermore, the interaction is voluntary, clear information is provided and there are alternative products such as physical newspapers that private individuals can view completely anonymously.

According to Bonnier News AB, the processing is unlikely to have a negative impact on the data subject's interest.

The processing that takes place lies within the data subject's reasonable expectations because the individuals who come into contact with the companies do so out of free will in order to access content on websites, purchase services and/or products and the fact that they always have a customer/user relationship with one or more of the companies within the Group. Furthermore, the companies' integrity policy contains clear information about how customers' and users' personal data are processed and shared within the Group. The processing carried out within the framework of the KDB/behavioural database is closely associated with the companies' services and products, which should have an impact on the consumer's expectations. The fact that a group coordinates systems and central functions and, as a consequence, shares certain data for reasons of efficiency should not be unexpected for data subjects. Customers who have not signed up to the NIX register have a reasonable expectation that their contact details may be used for postal direct marketing or telemarketing. Consumers are accustomed to this type of marketing.

The Group common policy provides information about direct marketing and telemarketing. It shows that addresses and telephone numbers can be used by the Bonnier companies for direct marketing via mail and telephone sales through tele marketing. It also appears that the Bonnier companies can choose segments that they believe are relevant to the campaign in question, e.g. 'men in the age range 40-45 years living in the Stockholm area'. It also shows that Bonnier companies always respect NIX-blocks and whether someone has objected to the marketing.

3.6.3 IMY's assessment

IMY deals with the first two steps in the balancing of interests test jointly for the supplemented and simple behavioural profiles (sections 3.6.4 and 3.6.5). The third and

final steps are then dealt with separately for the supplemented behavioural profiles (section 3.6.6) and the simple behavioural profiles (section 3.6.7).

3.6.4 Legitimate interest

There is a commercial aspect to Bonnier News AB's interest in creating profiles to make the data available to affiliated companies in order for them to be used in tele marketing and postal direct marketing. IMY considers that the companies' interest is lawful, real and actually. In light thereof, IMY considers that the company's interest in creating profiles to make data available to affiliated companies in order to be used in tele marketing and postal direct marketing is legitimate.

3.6.5 Is the processing necessary for the legitimate interest?

The necessity requirement in Article 6(1)(f) of the GDPR must be examined in conjunction with the principle of data minimisation set out in Article 5.³² The purpose of the processing is to make contact information available to companies to use in tele marketing and postal direct marketing. The supervisory case has revealed that Bonnier News AB, together with the other companies, has taken steps to minimise the number of data collected and limit how long this data is processed, as well as to ensure that the databases in which the data are processed are kept separate and that only certain data are transferred in between. Furthermore, the company has ensured that no more information than what is necessary is disclosed to the affiliated companies in order to be used in tele marketing and postal direct marketing. In light thereof, IMY considers that the processing is necessary for the legitimate purpose.

3.6.6 Balance of interests for the processing of personal data in supplementary customer database profiles

Bonnier News AB has emphasised that the affiliated companies have an interest in marketing their products and services in an efficient and privacy-friendly manner. However, IMY points out that the interest in making data available for use in tele marketing and postal direct marketing is a commercial interest that does not weigh particularly heavily.

In the assessment of the interests of data subjects, IMY considers the following:

The profiling carried out on the supplemented customer database profiles includes data collected from affiliated companies during purchases and subscriptions (so-called customer engagements), data collection from Bisnode Sverige AB and data from the behavioural database (including data collected by the affiliated companies through cookies). IMY has already stated that Bonnier News AB should not have a greater possibility than the affiliated companies to rely on legitimate interest for the processing of personal data collected by the affiliated companies using cookies. The behavioural data of the data subject collected from the behavioural database to KDB is collected from the websites of different companies. IMY believes that data subjects cannot reasonably expect their behavioural data to be collected for marketing purposes just because they visit a website. Nor can reasonably expect their behavioural data to be combined with data from another purchase or collected data from other records for the purpose of being contacted for tele marketing or postal direct marketing. This does not change by the fact that the privacy-enhancing measure that the affiliates carrying out the marketing action do not have access to the collected behavioural data, but only contact details.

³² See judgment in Asociația de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064, paragraph 48

The EDPB guidelines show that the scope of legitimate interest as a lawful basis for profiling depends on the level of detail of the profile, the size of the profile, the impact of profiling and the safeguards designed to ensure a fair, non-discriminatory and accurate profiling process.

IMY considers that the privacy interest of data subjects is strong due to the nature of the data, as the data enables the identification of individuals' behaviour and the collection of the data is given special protection in LEK.

IMY further points out that this is profiling within the meaning of Article 4(4) of the GDPR and that profiling is extensive as it provides in-depth insight on the data subject. There is also the fact that these are data collected from different websites combined with data collected from customer engagements and statistical data from Bisnode Sverige AB. In light thereof, IMY notes that the nature of the processing means that the privacy interest of the data subjects weighs heavily.

In conclusion, IMY considers that the data subject's privacy interest outweighs Bonnier News AB's and affiliated companies' interest in the processing of personal data that is based on so-called supplemented customer database profile and that is done in order to make contact information available to affiliated companies for tele marketing and postal marketing.

In light thereof, IMY points out that Bonnier News AB has processed personal data without having a lawful basis for doing so pursuant to Article 6(1) GDPR by profiling the data subjects based on their supplemented customer database profiles in order to make contact information available to affiliated companies for tele marketing and postal marketing.

3.6.7 Balance of interests for personal data not linked to the behavioural database

As IMY stated above in section 3.6.6, Bonnier News AB's interest is primarily a commercial interest that does not weigh particularly heavily.

As regards the assessment of data subjects' interests in processing operations unrelated to the behavioural database, IMY takes into account the following: Bonnier News AB has taken steps to minimise the number of data points both in relation to the principles of data minimisation and storage minimisation by not sharing data at object level, but only by product category, brand and type of packaging. Profiling also does not include data collected through cookies. The investigation has also shown that the data subject has been given the opportunity to object before the processing is conducted and that Bonnier News AB respects the data subjects' wishes to avoid marketing that has been noted in national block lists or with the controller. In light thereof, IMY considers that the processing is within what private individuals can reasonably expect from the information provided and that the contact information is disclosed only to affiliated companies within the Group.

In conclusion, IMY considers that the interests or fundamental rights of the data subjects do not outweigh the interests of Bonnier News AB and the affiliated companies for the processing in question.

In light thereof, IMY notes that Bonnier News AB can rely on Article 6(1)(f) of the GDPR for the processing in question.

3.7 Choice of corrective measure

3.7.1 Applicable provisions etc.

In case of violations of the GDPR, IMY has a number of corrective powers, including reprimand, injunction and administrative fines. This follows from Article 58(2)(a) to (j) of the GDPR. IMY shall impose administrative fines in addition to or in place of other remedies referred to in Article 58(2), depending on the circumstances of each case.

If a controller or processor, with respect to one or the same or linked data processing operations, intentionally or negligently infringes several of the provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount determined for the most serious infringement. This is stated in Article 83(3) of the GDPR.

Each supervisory authority shall ensure that the imposition of administrative fines on a case-by-case basis is effective, proportionate and dissuasive. This is stated in Article 83(1) GDPR. Article 83(2) sets out the factors to be taken into account in order to determine whether an administrative pecuniary penalty is to be imposed and when assessing the amount of the fine.

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR aimed to create a harmonised methodology and principles for the calculation of fines.³³

In the case of a minor infringement, according to Recital 148 of the GDPR, instead of imposing a fine, IMY may issue a reprimand under Article 58(2)(b).

3.7.2 Same or interconnected data processing operations

In three cases above, IMY has assessed that Bonnier News AB had no lawful basis in Article 6(1) of the GDPR for its processing of personal data. IMY considers that these processing operations, all of which take place in the company's databases through profiling for marketing purposes, are linked within the meaning of Article 83(3) of the GDPR.

3.7.3 Administrative fine

IMY has assessed that Bonnier News AB has infringed Article 6(1) of the General Data Protection Regulation in its processing of personal data that takes place for the purpose of displaying personalised advertisements and to make contact information available to affiliated companies for tele marketing and postal direct marketing. IMY does not consider these to be minor infringements. Bonnier News AB shall therefore be subject to an administrative fine for these infringements.

IMY notes that breaches of Article 6(1) of the GDPR fall within the scope of Article 83(5), which means that an administrative fine of up to 20 million EUR or 4 % of the global annual turnover in the previous financial year, whichever is the highest, may be imposed.

In determining the maximum amount of an administrative fine to be imposed on a company, the definition of 'company' used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR). It

³³ EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR (adopted for public consultation on 12 May 2022).

is clear from the Court's case-law that this applies to any entity engaged in an economic activity, irrespective of its judicial form and the means in which it is financed, and even if, in the judicial sense, the entity consists of several natural or legal persons.³⁴

IMY assesses that the company's turnover to be used as a basis for calculating the administrative fine imposed on Bonnier News AB is Bonnier News AB's parent company Albert Bonnier AB. The information gathered shows that Albert Bonnier AB's annual turnover in 2021 was 23 299 000 000 SEK. The maximum amount that can be determined for the administrative fine in the case is four per cent of this amount, i.e. approximately 931 960 000 SEK.

IMY considers that the following factors are relevant for the assessment of the gravity of the infringement.

There has been a matter of profiling of private individuals for profit when the profiling has been carried out in order to display personalised advertisements as well as when it has been used to provide contact details for tele marketing and postal marketing.

The profiling that has been used to show personalised ads has, in cases where data in the behavioural database about private individuals' browsing behaviour have been linked to KDB, included browsing history, purchase history and demographic and statistical data. It has been a matter of an ongoing infringement involving a large number of data subjects and covering a large amount of personal data. However, the data processed do not constitute, as far as IMY has found, special categories of personal data as set out in Article 9 of the GDPR. In this decision, IMY considered that the profiling through supplementary behavioural profiles was extensive in nature.

Regarding the profiling of personal data in KDB where there was a link to data in the behavioural database, so-called 'supplemented customer database profiles', IMY has assessed that the profiling was extensive in nature, since it contained data collected about the private individual's browsing behaviour collected from several websites combined with data from purchases made (customer engagement) and data collected from Bisnode Sverige AB. However, IMY makes the assessment that the personal data processing at issue does not have major privacy implications for the data subjects. The impacts are considered moderate.

In both cases, IMY considers that the profiling carried out where data could be linked in the two databases, supplementary behavioural profiles and the supplementary customer database profiles, has a higher degree of gravity compared to the infringement related to the profiling carried out in the so-called 'simple behavioural profiles' for displaying personalised advertisements. IMY considers that the profiling that takes place in the so-called simple behavioural profiles for displaying personalised advertisements in itself constitutes grounds for an administrative fine, but that it has a lower degree of gravity than the infringements where a link between the different databases could be made. The reasoning behind this is that there is lesser data regarding the data subjects and that the natural person only can be identified indirectly. However, IMY takes into consideration that this infringement also includes systematic processing which has been ongoing for a long period of time and concerned a large number of data subjects.

³⁴ See judgment in Akzo Nobel, C-516/15, EU:C:2017:314, paragraph. 48

The measures taken by Bonnier to limit the infringement of the privacy of data subjects, in the form of retention periods, that data are not collected at product level, that no more data than necessary are disclosed to affiliated companies, have according to IMY, significantly reduced the gravity of the infringements. Also, the personal data has not been disclosed outside the Group. IMY has noted that Bonnier News AB has consistently taken steps to reduce the privacy infringement of the data subjects in its group common cooperation. This has also been taken into account when assessing the gravity of the infringements.

In the light of the above, IMY considers that all of these are infringements of lower seriousness. The starting point for the calculation of the administrative fine should therefore be low in relation to the current maximum amount.

In addition to the assessment of the gravity of the infringement, IMY must assess whether there are any aggravating or mitigating circumstances affecting the amount of the administrative fine. IMY considers that there are no additional aggravating or mitigating circumstances, other than those taken into account in the assessment of the seriousness above, which affect the amount of the fine.

In view of the gravity, aggravating and mitigating circumstances of the infringement and the high turnover in relation to the infringements found, IMY sets the administrative fine for Bonnier News AB at 13 000 000 SEK. IMY considers this amount to be effective, proportionate and dissuasive.

This decision has been taken by the Director-General [REDACTED] after a presentation by the lawyer [REDACTED]. In the final proceedings, the head of court [REDACTED] and the head of unit [REDACTED] also participated.

[REDACTED], 2023-06-26 (This is an electronic signature)

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Summary Final Decision Art 60

Investigation

EDPBI:SE:OSS:D:2023:817

Administrative fine

Background information

Date of final decision:	26 June 2023
Date of broadcast:	26 June 2023
LSA:	SE
CSAs:	NO, DK, FI, EE, DE
Legal Reference(s):	Article 4 (Definitions), Article 6 (Lawfulness of processing) Administrative fine.
Decision:	Cookies, Consumer protection, Advertising, Lawfulness of processing, Legitimate interest, Profiling
Key words:	

Summary of the Decision

Origin of the case

The controller is a parent company in a group that includes several entities operating in media industry. The affiliated companies collect personal data from their customers and people who visit the company's websites. The data collected is then transferred into two group common databases, one customer database and one behavioural database. These databases generate profiles of individuals. The data stored in the behavioural database is consequently processed for the purpose of displaying personalised content and personalised advertisements in the digital services of the affiliated companies.

The LSA initiated supervision against the controller in order to investigate whether the controller complies with the GDPR requirements for the processing of personal data that takes place for marketing purposes pursuant to Article 6(1)(f) of the GDPR. The supervision covered the processing of personal data conducted through creating profiles and making it available to affiliated companies to be used to display personalized advertisements. It also covered the processing of personal data, the creation of profiles and the making available of data to affiliated companies in order to be used by affiliated companies in telemarketing and postal direct marketing.

Findings

The LSA made the assessment that the company in question is a joint controller of the data along with the affiliated companies for the part of the personal data processing that takes place for the common purposes

of making personal data available. Both when it comes to the legal basis for processing for the purpose of displaying personalised advertisements based on data in the behavioural database and the legal basis for processing for the purpose of making contact information available for telemarketing and postal direct marketing, the controller stated that the activities within the group have been coordinated in order to achieve a better data collection and make it possible to process the personal data for specified purposes in a cost-effective and integrity-friendly manner. The controller thus relied on the legal basis of Article 6(1)(f) of the GDPR for this processing of personal data.

The LSA stated that supplementary behavioural profiles do constitute **personal data** and even the simple behavioural profiles not linked to the controller's database mean that individuals are identifiable.

The LSA also found that that (1) the processing, both based on simple behavioural profiles and supplemented behavioural profiles that took place for the purpose of making the data available to affiliated companies for the purpose of displaying personalised advertisements and (2) that the processing for the purpose of making available contact details for telemarketing and postal direct marketing, included **profiling** of data subjects as defined in Article 4(4) of the GDPR.

When assessing reliance on the legal basis of **Article 6(1)(f)** of the GDPR, the LSA first noted that the controller has defined an interest that is legitimate. Second, the LSA concluded that the processing in question could be considered as necessary for the purpose stated by the controller. Third, the LSA assessed the balancing test and noted that the possibility for using Article 6(1)(f) GDPR as the lawful basis for profiling based on observed data is limited. The LSA further stated that the privacy interest of data subjects is of great significance due to the nature of the data. The LSA noted that in this case the profiling included data collected from other contexts such as previous purchases, collected demographic data and statistical data. The LSA further considered that profiling was extensive in its nature and that such profiling was not something a data subject could expect without having consented to such processing of personal data. In conclusion, LSA considered that because the processing enabled profiling of individuals, the data subject's privacy interest outweighed the interests of controller and affiliated companies.

In light thereof, LSA found that the controller has processed personal data without having a lawful basis pursuant to Article 6(1) GDPR in order to profile the data subjects based on their behavioural data in a so-called supplemented behavioural profile and make the profiles available to affiliated companies in order to display personalised advertisements. In addition, the LSA found that the controller has processed personal data without having a lawful basis pursuant to Article 6(1) GDPR in order to profile the data subjects based on their behavioural data in so-called simple behavioural profiles and make the profiles available to affiliated companies for the purpose of displaying personalised advertisements and by profiling the data subjects based on their supplemented customer database profiles in order to make contact information available to affiliated companies for tele marketing and postal marketing.

When it comes to processing of personal data not linked to the behavioural database, the LSA noted that the controller has taken steps to minimise the number of data points both in relation to the principles of data minimisation and storage minimisation and that profiling did not include data collected through cookies. Also, the investigation has shown that the data subjects have been given the opportunity to object before the processing was conducted and that the controller respected the data subjects' wishes to avoid marketing that has been noted in national block lists or with the controller. In conclusion, LSA considered that the interests or fundamental rights of the data subjects did not outweigh the interests of the controller and it could indeed rely on Article 6(1)(f) of the GDPR for the processing in question.

Decision

Pursuant to Articles 58(2) and 83 of the GDPR, in view of the gravity, aggravating and mitigating circumstances of the infringement and the high turnover in relation to the infringements, the LSA ordered the controller to pay an administrative fine of SEK 13.000.000 (approximately EUR 1.150.000). The LSA considered this amount to be effective, proportionate and dissuasive.

Summary Final Decision Art 60

Complaint

EDPBI:SE:OSS:D:2023:824

Administrative fine; Compliance order

Background information

Date of final decision:	30 June 2023
LSA:	SE
CSAs:	DE, NO, DK, EE, PT, ES, FI, AT
Legal Reference(s):	Article 44 (General principle for transfers), Article 4 (Definitions), Article 46 (Transfers by way of appropriate safeguards) Ref 4 (if any).
Decision:	Compliance order, Administrative fine.
Key words:	International transfer, Third party access to personal data, Administrative fine, Cookies, Definition of personal data

Summary of the Decision

Origin of the case

On the basis of a complaint that the LSA received against the controller regarding transfers of personal data to a third country under Chapter V of the GDPR, the LSA initiated supervision against the controller.

In the complaint of 14 August 2020, the complainant submitted that the controller, through the use of an analytics tool implemented on its website, was transferring the complainant's personal data to third countries without fulfilling the conditions laid down in Chapter V of the GDPR. According to the complainant, with the analytics tool implemented on the controller's website, the transfer of the complainant's personal data to the data processor established in the United States of America took place, when the complainant visited the controller's website.

The LSA investigated whether the controller had transferred personal data to the United States of America within the framework of the analytics tool, and whether the controller had done so in accordance with Chapter V of the GDPR.

Findings

The LSA found that, in light of the unique identifiers and the possibility of combining these with additional data, the controller was processing personal data through the analytics tool.

The LSA also found that the personal data collected through the tool was stored by the data processor in the United States of America. For this transfer, the controller and processor had relied on the European Commission's Standard Contractual Clauses within the meaning of Article 46 of the GDPR. However, the LSA noted that following the judgment by the Court of Justice of the European Union ("CJEU") in C-311/18 (Schrems II), and based on the recommendations of the European Data Protection Board on the consequences of the judgment, the use of the Standard Contractual Clauses may require supplementary measures. The LSA then noted that, in order to determine whether such supplementary measures would be necessary, an analysis of the legislation of the third country in question needed to be carried out. With reference to the assessment of the legal situation in the United States of America conducted by the CJEU in Schrems II, the LSA found that the use of the Standard Contractual Clauses was not in itself sufficient to achieve an acceptable level of protection for the transferred personal data.

Then, the LSA assessed whether the controller had taken supplementary measures to ensure the effectiveness of the Standard Contractual Clauses. The LSA considered the measures implemented by both the controller and processor and found that the supplementary measures implemented by the controller and processor were not effective, as they did not prevent the US Intelligence Services from accessing the personal data or rendering such access ineffective. The LSA considered that neither the Standard Contractual Clauses nor the supplementary measures implemented could support the transfer as set out in Chapter V of the GDPR. On this basis, the LSA found that the controller undermined the level of protection of personal data guaranteed by Article 44 of the GDPR.

Decision

The controller was found to have processed personal data in breach of Article 44 of the GDPR. The LSA noted that the controller had transferred a large amount of personal data, that the processing had been going on for a long time and that the transfer meant that the personal data was not guaranteed the level of protection afforded in the EU/EEA but also that the controller had taken some measures, albeit insufficient, to try to limit the transfer. The LSA concluded that the controller should pay an administrative fine of SEK 300.000 (approximately EUR 25.600). Further, the LSA ordered the controller to discontinue the use of the version of the analytics tool used on 14 August 2020, unless appropriate safeguards were put in place. The LSA ordered to implement these measures no later than one month after the decision had become final.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's draft decision.

COMPLAINANT

See appendix

Swedish ref no:
IMY-2023-15896**Nat.ref.no**
2023-31-7819**IMI case register:**
580527**Date of the decision:**
2024-07-31**DATA CONTROLLER**
Scandinavian Airlines System AB

Final decision under the General Data Protection Regulation – Scandinavian Airlines System AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Scandinavian Airlines System AB has processed personal data in breach of Article 12 (3) of the General Data Protection Regulation (GDPR)¹ by not having accommodated the complainant's request for erasure made on the 1 September 2019 without undue delay, and first on 15 June 2023.

The Swedish Authority for Privacy Protection issues a reprimand to Scandinavian Airlines System AB pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(3) of the GDPR.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision against Scandinavian Airlines System AB (SAS) due to a complaint. The complainant has been submitted to IMY, as the lead supervisory authority under Article 56 of the GDPR, by the supervisory authority of the country (Denmark) in which the complainant lodged its complaint in accordance with the Regulation's provisions on cooperation in cross-border processing.

Since it is a cross-border complaint, IMY has made use of the mechanisms for cooperation and consistency of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Netherlands, Belgium, Estonia, France, Norway, Germany (Bayern, Berlin, Hesse) and Ireland.

The complainant has stated the following. The complainant requested access to his personal data on 1st September 2019. The complainant received an email from SAS

Postal address:
Box 8114
104 20 Stockholm**Website:**
www.imy.se**E-mail:**
eu@imy.se**Telephone:**
08-657 61 00

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).

that the request will be complied within 30 days. The complainant's request was complied with on the 15th June 2023.

SAS has stated the following. SAS received the complainant's request for access on 1 September 2019. As of September 6, 2019, SAS systems that manage data subjects' rights and access to information ("Privacy App"), have collected all necessary data. Normally, the Privacy App sends an email to the individual who requested their information, but in this specific case the email function in the system was not working. Only one data subject, the complainant in this case, was affected by this. In 2023, the Privacy App was updated and changes were made to the email function, which is the reason that the system sent the delayed response to the complainant. SAS had no knowledge that the complainant had not previously received a response from the Privacy App.

Since May 2018, the Privacy App has produced information about 1,300 times, and SAS review the functionality and process of this procedure at least once a year. This is the first time that this technical bug has been found in the Privacy App, and this bug is now fixed.

SAS believes that they have handled the request from the data subject on time, but that unfortunately there was a technical bug in the Privacy App that SAS did not know about at the time, which meant that the email response to the complainant (that SAS had no information about the complainant) got stuck in the Privacy App.

The complainant has been given the opportunity to comment on the material but has not been heard.

Applicable provisions, etc.

It follows from Article 57(1)(f) of the GDPR that IMY shall handle complaints lodged by a data subject who consider that their personal data is being processed in a manner contrary to the Regulation and investigate, to the extent appropriate, the subject matter of the complaint. The Court of Justice of the European Union has ruled that the supervisory authority must investigate such complaints with due care.²

Pursuant to Article 15 of the GDPR, a data subject has the right to obtain from the controller confirmation as to whether or not personal data relating to him or her are being processed and, if so, access to the personal data and certain information.

Pursuant to Article 12(3) of the GDPR, upon request, the controller shall provide the data subject, without delay and in any event no later than within one month of receipt of the request, with information on the measures taken pursuant to, inter alia, Article 15 of the GDPR. That period may be extended by two months further, if necessary, considering the complexity of the request and number of requests received. The controller shall inform the data subject of such an extension within one month of receipt of the request and shall state the reasons for the delay.

Assessment of IMY

It appears from the investigation that the parties agree that the complainants request for access was complied with more than one month after the request was received. It does not appear that the request was of a particularly complex nature. Nor is it

² Schrems II, C-311/18, EU:C:2020:559, p. 109.

apparent that SAS informed the applicant of the delay in accordance with Article 12(3) of the GDPR. IMY therefore takes the view that SAS failed to fulfil their obligation under Article 12(3) of the GDPR in that they did not comply with the complainants request to access on the 1 September 2019 until the 15 June 2023.

Choice of corrective measure

It follows from Article 58(2) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines pursuant to Article 83 of the GDPR.

In the case of a minor infringement, the IMY may, as stated in recital 148 of the GDPR, instead of imposing a pecuniary penalty, issue a reprimand pursuant to Article 58(2)(b) of the GDPR. Account must be taken of aggravating and mitigating circumstances of the case, such as the nature, severity and duration of the infringement as well as previous relevant infringements.

IMY notes the following relevant circumstances. The supervision covers SAS handling of an individual complainants request for access to his personal data. The infringement in question has affected one person and has occurred due to a temporary system problem at SAS. The company states that this is the first time that the technical bug occurred and that it has now been fixed. Against that background, IMY considers the infringement to be minor within the meaning of recital 148 and that Scandinavian Airlines Systems AB should be issued a reprimand under Article 58(2)(b) of the GDPR.³

This decision has been made by specially appointed decision-maker, legal advisor [REDACTED] after presentation by legal advisor [REDACTED].

Appendix

The complainant's personal data

³ EDPB Guidelines 04/2022 on the calculation of administrative fines under the GDPR (finally adopted on 24 May 2023).

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2024-07-29, no. IMY-2023-16127. Only the Swedish version of the decision is deemed authentic.

Diarienummer:
IMY-2023-16127

Ref no:
IMY-2023-16127
IMI case no CR 595291

Date of translation :
2024-07-29

Final decision pursuant to Article 60 under the General Data Protection Regulation – Ellos Group AB and Ellos Group Sweden AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Ellos Group Sweden AB in its handling of the complainant's request for access made on 25 August 2020 has processed personal data in breach of Article Article 12(3) of the GDPR by failing to comply with the complainant's right of access under Article 15 of the GDPR without undue delay.

The Swedish Authority for Privacy Protection closes the part of the supervision that has been directed at Ellos Group AB.

Presentation of the supervisory case

IMY has received a complaint against Ellos from the Danish Supervisory Authority (Datatilsynet) in accordance with the provisions on the competence of the lead supervisory authority in Article 56 GDPR.

The case has been handled through written procedure. In the light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authority concerned have been the data protection authority in Denmark.

The deficiency in question alleged in the complaint is that the complainant did not obtain access to its data in a timely manner and that the copy of the data was not complete.

IMY initiated supervision and sent our questions to Ellos Group AB.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Ellos Group Sweden AB is the data controller for the processing of personal data described in the complaint. The company received the applicant's request for access by e-mail on 25 August 2020. Requests for access were received through a channel that normally handles other types of issues and is not monitored as regularly as the

channels referred to for these types of requests. The complainant's request was therefore left unaddressed for a longer period than desirable and was not dealt with within the time limit. The access request was handled by email on 22 December 2020.

On 24 December 2020, the complainant submitted a request for further information. On 7 January 2021, Ellos Group Sweden AB informed the complainant that the requested information was processed by Resurs Bank as data controller. Ellos Group Sweden AB considers that the information provided to the complainant was complete.

The complainant, through the Danish supervisory authority, has been given the opportunity to comment on Ellos Group Sweden AB's reply, but has not submitted any comments.

Statement of reasons for the decision

As defined in Article 4(7) of the GDPR, the controller is the person who alone or jointly with others determines the purposes and means of the processing of personal data. Ellos Group Sweden AB has stated that Ellos Group Sweden AB is the data controller for the personal data processing to which the complaint relates and not Ellos Group AB to which the first supervisory letter was addressed. Against this background, IMY concludes that Ellos Group Sweden AB is the data controller for the current processing of personal data, which is why the supervisory case directed against Ellos Group AB hereby is closed.

The controller shall be obliged to inform any person who so requests whether or not personal data relating to the applicant are being processed. Where such data are processed, the controller shall, in accordance with Article 15 of the GDPR, provide the data subject with supplementary information concerning, inter alia, the purposes of the processing and the recipients of the data, as well as a copy of the personal data processed by the controller.

The investigation in the case shows that Ellos Group Sweden AB received the complainant's first request for access on 25 August 2020 and that the complainant's request was complied with on 22 December 2020. IMY finds that Ellos Group Sweden AB has processed the complainant's personal data in breach of Article 12(3) of the GDPR by failing to comply with the complainant's request for access pursuant to Article 15 of the GDPR without undue delay, or at the latest within one month.

The investigation also shows that the company received the applicant's request for additional information on 24 December 2020. Ellos Group Sweden AB has stated that current data is processed by Resurs Bank and that the company provided information about this to the complainant on 7 January 2021. The investigation has not revealed any reason to question that Ellos Group Sweden AB is not the data controller for the processing in question. In those circumstances, IMY finds that the investigation does not show that the applicant's personal data were processed in breach of Article 15 of the GDPR.

Choice of corrective measure

Within the scope of the corrective powers, IMY shall take such measures as are appropriate, necessary and proportionate to ensure compliance with the GDPR.

It follows from Article 58(2) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83 of that regulation. In the case

of a minor infringement, IMY may, as stated in recital 148 of the GDPR, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements, must be taken into account. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The current supervision covers Ellos Group Sweden AB's handling of an individual complainant's request for access in the light of the requirements set out in Article 12(3) of the GDPR. In doing so, IMY has found that Ellos Group Sweden AB has failed to fulfil its obligations to fulfil the right in time. The prescribed time limit of a maximum of one month has been exceeded by just under three months. However, the applicant's right of access has been granted. The deficiencies found are therefore of a less serious nature than if the request had been left unanswered. In addition, the request had already been accommodated long before IMY contacted Ellos Group Sweden AB with questions about the complaint in question. Furthermore, the infringement was not intentional.

On an overall assessment of the circumstances of the infringement found, IMY concludes that there is no need to use the corrective powers in the present case.

The case should therefore be closed.

[REDACTED], 2024-07-29

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Rusta AB

Swedish ref. number:
IMY-2022-2745

Norwegian ref. number:
20/03594

IMI case register:
355627

Date:
2024-08-23

Final decision under the General Data Protection Regulation – Rusta AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Rusta AB (556280-2115) has processed the complainant's personal data in breach of:

- Article 17(1)(c) GDPR by not erasing the personal data of the complainant after the complainant objected to the processing of his personal data for direct marketing purposes in accordance with Article 21(2)
- Article 21(3) of the GDPR by not having ceased to process the complainant's personal data for direct marketing purposes following the complainant's objection to the processing.

IMY issues a reprimand to Rusta AB pursuant to 58(2)(b) of the GDPR.

Presentation of the supervisory case

Processing

IMY has initiated a supervision against Rusta AB (Rusta or the company) due to a complaint. The complaint has been submitted to IMY as the lead supervisory authority under Article 56 GDPR. The handover has been made by the supervisory authority of the country where the complainant lodged his complaint (Norway) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The case has been handled through a written procedure. In view of the cross-border processing, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities of Norway, Finland and Denmark.

The complaint

The complainant essentially states that she received repeated text messages from Rusta asking her to register as a member. On the basis of the text messages, the complainant contacted Rusta by telephone and e-mail, and informed the company of the mailings and asked them to remove her number from their system. Nevertheless, the mailings have continued.

Rusta's statement

Rusta essentially states the following. The company is the controller for the processing to which the complaint relates. The complainant contacted the company on five occasions and requested erasure. The data has been deleted at all times. Rusta only sends this type of communication to people who have actively chosen to join Rusta's customer club (Club Rusta) by providing their mobile number when purchasing from Rusta. If a person – after providing their mobile number – does not complete their registration within 30 days, the mobile number is automatically deleted. In addition to automatic deletion, Rusta has the option to manually delete the mobile number from Rusta's system.

If someone contacts Rusta to be removed from mailings, Rusta's routine is that personal data is deleted from Rusta's system. As shown in the supplier's description, erasure means that Rusta stops processing the personal data and that Rusta does not send any further communication. Since Rusta deleted the personal data of the data subject on each occasion, the company has therefore ceased the processing of this data for direct marketing purposes.

In order for someone, after erasure, to receive communication from Rusta, someone must re-enter the mobile number when making a purchase at Rusta. This is possible because Rusta does not retain any data after deletion. Rusta does not keep any technical logs that show that erasure has occurred. However, Rusta has provided messages from Rusta's customer service confirming erasure. Furthermore, the employees who worked in Rusta's customer service at the time of the relevant requests can confirm that the erasure took place.

The probable reason why the data subject has continued to receive mailings is that someone has repeatedly provided the data subject's mobile number when purchasing from Rusta. This may have been because someone mistakenly perceived that the complainant's mobile number was their own, or intentionally used the complainant's mobile number, for example to receive membership benefits without registering themselves.

The reason why the data subject has received communication from Rusta (after objection) is that the data subject's mobile number has been provided again when purchasing from Rusta, not that Rusta has resumed communication based on existing personal data. Rusta's assessment has been that it is not in compliance with the GDPR to create 'block lists' to prevent future communications. No reprimand should be issued as it would be disproportionate.

Rusta has been given the opportunity to comment on IMY's draft decision.

Rusta has attached a description of the flow for registering and deleting contacts in the system used by the company.

Motivation for the decision

The issue in the case

The examination in this supervision concerns whether Rusta has complied with the complainant's request to have its telephone number removed from the company's system to stop mailings. In this supervision, IMY has not taken a position on any requirements to prevent future mailings.

Right to object to direct marketing

According to Article 21(2) of the GDPR, the data subject shall have the right to object at any time to processing of personal data concerning him or her for direct marketing purposes. Furthermore, as stated in the Article 21(3) of the GDPR, personal data shall no longer be processed for such purposes if a data subject objects to the processing.

The investigation in the case shows that Rusta sent text messages to the complainant with a link to confirm membership of the customer club. The mailings were sent via a direct channel to the complainant from the company with information on how to complete the registration to the customer club. IMY considers that this type of mailing constitutes direct marketing since it is sent directly to the complainant for a commercial purpose.¹ Therefore, there has been a right for the complainant to object to this processing of personal data under Article 21(2) GDPR.

On five separate occasions, the complainant asked Rusta to erase her number from their system because she did not wish to receive text messages and also stated that she had not registered with the customer club. The complainant has therefore expressly requested erasure. The question, however, is whether her request for erasure should also be considered to include an objection to direct marketing.

The European Data Protection Board (EDPB) Guidelines 01/2022 on the rights of data subjects (right of access) state:

It should be noted that the GDPR does not introduce any formal requirements for persons requesting access to data. In order to make the access request, it is sufficient for the requesting persons to specify that they want to know what personal data concerning them the controller processes. Therefore, the controller cannot refuse to provide the data by referring to the lack of indication of the legal basis of the request, especially to the lack of a specific reference to the right of access or to the GDPR.

[...]

It should be borne in mind that complainants may not be familiar with the intricacies of the GDPR and that it is advisable to be lenient towards persons exercising their right of access.²

IMY's assessment is that the responsibility of the controller to give a broad interpretation of persons exercising their rights applies to all rights under the GDPR, not only to the right of access. It is therefore concluded that, even if the complainant

¹ Judgment of the Court of Justice of the European Union of 25 November 2021, Case C-102/20, paragraph. 47.

² EDPB Guidelines 01/2022 on data subject rights – Right of access, Version 2.0, (finally adopted on 28 March 2023), para. 50.

has not expressly invoked Article 21, her letters should nevertheless be interpreted, taking into account the circumstances, as an objection to direct marketing in accordance with Article 21(2) GDPR. The complainant's intention must, in the circumstances of the case, be deemed to have been to object to the direct marketing.

The consequence for the controller when a data subject has objected to a processing with the purpose of direct marketing is that the personal data shall no longer be processed for such purposes. Rusta should therefore have ceased the processing of the complainant's personal data for direct marketing purposes when she made her first objection. The complainant shall not have to repeat its objection on several occasions in order for the company to cease the processing of personal data. However, the investigation in the case shows that the complainant continued to receive text messages from Rusta despite her objections and that the company therefore continued to process the complainant's personal data for direct marketing purposes. IMY finds that Rusta has therefore acted in breach of Article 21(3) of the GDPR.

Right to erasure

According to Article 17(1)(c) GDPR, 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 if the data subject objects to the processing pursuant to Article 21(2).

The investigation in the case shows that on five separate occasions the complainant contacted Rusta and requested the company to erase her phone number. As noted above, and for reasons set out therein, the complainant's request for erasure must be considered to include an objection pursuant to Article 21(2) GDPR.

Rusta states that on all five occasions the company erased the complainant's telephone number within 24 hours. However, the investigation in the case shows that the complainant has continued to receive text messages from Rusta despite the fact that the erasure of the complainant's telephone number is said to have taken place. IMY considers that the explanation given by Rusta as to why the complainant continued to receive text messages, specifically that incorrect numbers may have been provided by another customer at the checkout, or that employees at the checkout may have accidentally entered an incorrect number, does not appear likely. If that were the case, the error must have occurred on five separate occasions. Instead, according to IMY, it is clear from the circumstances of the case that Rusta has not been able to completely fulfil the complainant's right to erasure. IMY finds that Rusta has therefore acted in breach of Article 17(1)(c) of the GDPR.

Summary

In summary, IMY notes that the investigation in the case shows that Rusta processed the complainant's personal data in breach of Article 17(1)(c) of the GDPR by not erasing the complainant's personal data following the complainant's objections under Article 21(2) and that Rusta processed the complainant's personal data in breach of Article 21(3) of the GDPR by not having ceased to process the complainant's personal data for direct marketing purposes following her objections to the processing.

Choice of corrective measure

According to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case need to be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The current supervision includes an examination of how Rusta has handled one person's request for erasure and objection. IMY finds that Rusta has failed to fulfil its obligations under those rights towards the complainant. Rusta has however taken measures, even if they prove to be insufficient, in order to comply with the complainant's request for erasure and objection. The present deficiencies are therefore of a less serious nature than if the request had been completely disregarded. Rusta has also stated that they have an ongoing investigation to review the possibility of blocking phone numbers from being registered, or receiving SMS mailings. The company has not previously been found to have infringed the General Data Protection Regulation.

Against this background, IMY considers that these breaches are minor infringements within the meaning of recital 148 and that Rusta AB is to be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

COMPLAINANT

See appendix

Registration number::
IMY-2023-16503

DATA CONTROLLER
Klarna Bank AB

Case register/National registration number:
CR 134712
521.14296 / 631.370

Date:
2024-09-05

Decision under the General Data Protection Regulation – Klarna bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) notes that it is not apparent from the investigation in the case that Klarna Bank AB (org. no. 556737-0431) has failed to comply with¹ the GDPR in the manner stated in the complaint.

The case is closed.

Presentation of the supervisory case

The Privacy Protection Authority (IMY) has received a complaint regarding the right to information pursuant to Article 13 of the GDPR and the right of access pursuant to Article 15 of the GDPR and initiated supervision of Klarna Bank AB (Klarna or the Company). The complaint has been submitted to IMY by the supervisory authority of the country where the complainant lodged its complaint (Germany) in accordance with the Regulation's provisions on cooperation in cross-border processing. IMY has dealt with the complaint as the lead supervisory authority under Article 56 GDPR.

The proceedings at IMY have been carried out by exchange of letters. In view of the cross-border processing, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The relevant supervisory authorities have been the data protection authorities of Germany, Austria, Hungary, Denmark, Norway, Finland, Italy, the Netherlands, Poland, Ireland, France, Estonia and Spain.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

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).

The appellant states, in essence, as follows. By e-mail from Klarna on 13 August 2021, the complainant received information that a register extract was sent to the complainant by post. The extract of the register reached the complainant on 17 August 2021. The complainant lacks information on the legal basis for the processing of his or her personal data and what personal data have been processed.

Klarna states, in essence, the following. On 18 January 2021, Klarna received the complainant's request for the personal data processed. At the same time, they received questions from the complainant concerning the processing of personal data, but the legal basis is not asked about there. Klarna replied to the other questions put by the appellant. Klarna further states that if the complainant has further questions about the processing, the complainant is welcome to contact Klarna again. On 5 February 2021, Klarna referred by e-mail to the extract from the register which, in accordance with the applicant's request, was subsequently sent by post to the applicant on 8 February 2021 for answers to the complainant's questions. The legal basis for the processing has been specified in this extract. The appellant has not returned after that. Klarna has further stated that the legal basis per purpose is set out in Klarna's data protection information (including for each recipient).

The appellant has been given the opportunity to comment on Klarna's reply but has not submitted observations.

Statement of reasons for the decision

It follows from Article 57(1)(f) of the GDPR that the IMY shall deal with complaints from data subjects who consider that their personal data are being processed in a manner contrary to the Regulation. It also follows from that provision that, where appropriate, IMY must examine the subject matter of the complaint. The CJEU has ruled that the supervisory authority must investigate such complaints with due care.²

According to Section 23 of the Swedish Administrative Procedure Act (2017:900), an authority must ensure that a case is investigated to the extent required by its nature.

The right to information derives from Article 13 of the GDPR. Article 13(1)(c) provides that the data subject has the right to obtain from the controller information about the purposes of the processing for which the personal data are intended and the legal basis for the processing. The right of access follows from Article 15 of the GDPR. The provision means that the data subject shall have the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed and, if so, to have access to the personal data as well as certain supplementary information, including the purposes of the processing.

In response to the complaint, IMY has put a number of questions to Klarna. IMY then gave the appellant the opportunity to comment on Klarna's answer to IMY's questions. IMY considers that through these measures the case has been investigated to the extent required by Article 57(1)(f) of the GDPR and Section 23 of the Swedish Administrative Procedure Act.

² Judgment in Schrems II, Case C-311/18, EU:C:2020:559, paragraph 109.

The appellant submits, in essence, that Klarna did not provide information on which personal data were processed or on the basis of the legal basis on which the personal data were processed. In the course of the investigation of the complaint in response to IMY, Klarna stated that it responded to the applicant's request for access and that, according to Klarna, the extract of the register sent to the applicant on 8 February 2021 specified the legal basis for the processing. The appellant has been given the opportunity to comment on Klarna's statement but has not been heard. IMY finds that it is not possible to conclude from the investigation in the case that Klarna has failed to comply with the GDPR on what is claimed in the complaint.

The case should therefore be closed.

This decision has been taken by the senior legal advisor [REDACTED], after presentation by legal advisor, [REDACTED].

Annex

Personal data of the complainant

Copy

The company's DPO

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

COMPLAINANT

See appendix

Registration number:
DI-2021-5451

DATA CONTROLLER
Ellos Group AB

Case register/National registration number:
CR 155123
4098/182/2018,
801/163/2019

Date:
2024-09-03

Decision under the General Data Protection Regulation– Ellos Group AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Ellos Group AB (org. nr. 556217-1925) has processed the complainant's personal data in any event during the period from 6 July 2018 to 30 June 2021 in breach of Article 32 of the GDPR¹ by failing to take appropriate technical and organisational measures to ensure adequate protection against unauthorised disclosure on its website of personal data in the complainant's customer profile.

The Swedish Authority for Privacy Protection issues a reprimand to Ellos Group AB pursuant to Article 58(2)(b) of the GDPR for breach of Article 32 of the General Data Protection Regulation.

Presentation of the supervisory case

Handling of the case

The Swedish Authority for Privacy Protection (IMY) has initiated a supervision regarding Ellos Group AB (Ellos) due to two complaints. The complaints have been submitted to IMY, as lead supervisory authority under Article 56 GDPR. The handover has been made from the supervisory authority of the country where the complainants has lodged their complaints (Finland) in accordance with the provisions of the GDPR on cooperation in cross border processing.

The case has been handled through written procedure. In the light of the complaint concerning a cross border processing, IMY has used the mechanisms for cooperation

Postal address:
Box 8114
104 20 Stockholm, Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

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)

and consistency contained in chapter VII of the GDPR. The supervisory authorities concerned have been the Finnish Authority for Privacy Protection.

The complaints

The complainant has mainly stated the following. The complaints allege a security flaw on the websites of Ellos, Ellos and Jotex online store (ellos.fi and jotex.fi). The complainants have observed that it was possible for them to log in to the Ellos online store using only email and postcode. Thus, no password or other verification method was needed for login. After the complainants have logged in with the new method, you can see the individual's profile including; telephone number and address and the nearest delivery point. Even if the address is partly hidden, it is not difficult to guess the correct address with the help of the nearest delivery point. One of the complaints also states that it is possible to see the individual's purchase history.

What Ellos has stated

Ellos Group AB has mainly stated the following.

Ellos is the controller of the processing operations to which the complaint relates.

The login method to which the complaints relate is referred to as 'soft log-in'. It is a simplified login to Ellos and Jotex online stores that allows the customer to access certain features of the online store. The simplified login is a common solution in the industry with the aim of providing benefits to already registered customers by facilitating their purchase process.

Through soft log-in it is possible to place orders for products in the online store. At the checkout, the customer can see their pseudonymised information about their name, address and telephone number, as well as information about possible delivery points. Pseudonymisation means that the data can only be identified by someone who already has knowledge of the complete data. In addition to this, no access to purchase history and other customer data is given at soft log-in. Access to purchase history and other customer information requires the customer to make a full login with password.

Before placing an order, there is a clear request to the customer to ensure that the pseudonymised personal data displayed is correct. If the personal data is incorrect, there is a reference where the customer can log in to their customer account with a full login. When ordering, a confirmation email always goes to the email address registered in the account, so that the account holder has the opportunity to cancel the order if it has been made by the wrong person. Delivery can only be made to the address registered in the customer account or a delivery point. If delivery is made to a delivery point, the product cannot be collected without the registered customer's ID document. The customer always has the right of withdrawal if someone else has placed the order in the customer's name.

In summary, there are a number of security measures built into the soft log-in process to prevent the wrong person from placing an order in the name of another customer, as well as to prevent an order from being placed by the wrong person. The risk that unauthorized use of someone else's customer account when ordering is completed to the detriment of the customer is thus limited. Overall, the requirement for appropriate security measures under the General Data Protection Regulation is met.

When asked how Ellos ensured, in relation to the complainants in the complaints, that the right persons had access to the data and ordered products when ordering over the internet, Ellos replied as follows.

As mentioned above, before placing an order, the complainants have been clearly instructed to ensure the accuracy of the pseudonymised personal data displayed. It is not apparent from the complaints that the complainants ordered any products. Ellos works continuously to review and evaluate its work processes and security measures to protect data subjects' personal data and to promote a safe customer experience on the internet.

Statement of reasons for the decision

Applicable provisions

Article 32 of the GDPR governs the security of processing. The controller shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons, take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In assessing the appropriate level of security, particular account shall be taken of the risks posed by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Assessment of IMY

The investigation in the case shows that Ellos uses a so-called 'soft log-in'. This is a login method that only requires the customer to provide their email address and postal code in order to access a part of their customer profile. The 'soft log-in' mode shows the customer's name, address, telephone number and the nearest delivery point. One of the complaints states that the customer's purchase history is also shown, but this is disputed by Ellos. There is no support in the investigation to question Ello's statements that purchase history is not shown after the 'soft log-in'.

When processing personal data, they shall be processed in a way that ensures appropriate security of the personal data based, inter alia, on their sensitivity. Personal data such as name, telephone number and address data are not sensitive data under Article 9 of the General Data Protection Regulation, nor are they particularly worthy of protection, such as personal identity numbers, nor so-called privacy-sensitive data. Current categories of data exist in some Member States in publicly available sources (including in Sweden with the exception of so-called protected personal data and in Finland with the possibility to request a ban on the disclosure of personal data).

Exposure of personal data on the internet is a particular risk in itself when the data is made available to an unlimited number of natural persons. The current risk is that people who do not want their data to be disseminated openly on the internet will still have their personal data exposed.

When processing personal data, they shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or

unlawful processing.² Authentication means that users confirm their declared identity. It is about ensuring that the right user has access to a user account or system.

Authentication can be done by the user entering their username and password in order to access a program, service or system.

Authentication is a two-step security measure. First, the user *identifies* themselves and then the user *verifies* the declared identity with some form of authentication tool, such as a password. In the described ‘soft log-in’ process, users identify themselves with their email address. However, no actual verification is carried out, as postal codes are publicly available information that can be accessed via, for example, the Finnish Post Office’s website (posti.fi). Postal codes can be linked to an individual and are neither ‘secret’ nor individual. The personal data contained in the ‘soft log-in’ customer profiles therefore lack authentication protection. The lack of protection means that people who do not want their data to be disseminated openly on the internet still risk having their personal data exposed.

Ellos has stated that the personal data on the website is pseudonymised.

Pseudonymisation is a security measure whereby personal data are processed in such a way that the personal data can no longer be directly attributed to a specific data subject without the use of additional data, provided that such additional data are kept separately and are subject to technical and organisational measures that ensure that the personal data are not attributed to an identified or identifiable natural person.

Pseudonymised personal data is still personal data, although the risk of identifying a person is reduced, as the possibility of identification still exists. From what has emerged from the complaints, the processing of personal data on Ellos website means that the address information is only partially hidden. It is possible with the help of the nearest delivery point, which is also shown on the website, to find the right address. Thus, additional data enabling the personal data to be attributed to a specific data subject are not kept separately. IMY therefore considers that the measure known as the pseudonymisation of Ellos is not such as to achieve an appropriate level of security in relation to the risk of the appellants’ personal data being exposed via the internet.

IMY considers that the appellants’ personal data have been exposed via the internet without adequate protection and, therefore, that the data have been made accessible to an unlimited number of natural persons. IMY notes that the measures taken by Ellos did not sufficiently reduce the exposure of the complainants’ personal data via the internet. It has thus not provided an appropriate level of security in relation to the risks posed by processing.

In conclusion, IMY finds that Ellos has not taken appropriate technical and organisational measures under Article 32 to ensure adequate protection against unauthorised disclosure on its website of personal data in the complainant’s customer profile. Ellos has thus processed personal data in breach of Article 32 of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as reprimand, injunctions and prohibitions. Furthermore, it is clear from Article 83(2) which factors

² Article 5(1)(f) GDPR

must be taken into account when deciding on an administrative fine and when determining the amount of the fine. Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The current supervision covers Ellos processing of complainants' personal data in the situation to which the complaint relates. The infringement was not intentional but negligent. Against that background, IMY considers that that infringement is not of such a nature that a fine should be imposed and that Ellos Group AB shall therefore be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been taken by Head of Unit, [REDACTED], after presentation by legal advisor, [REDACTED].

The IT and information security specialist [REDACTED] was also involved in the final processing of the case.

Appendix

The complainant's personal data 1
The complainant's personal data 2

Copy to:

The company's DPO

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

COMPLAINANT

See appendix

CONTROLLER

Warner Music Sweden AB

Swedish ref.:
IMY-2023-16448

National ref.:
D130.870

IMI case register:
388187

Date:
2024-10-04

Final decision under the General Data Protection Regulation – Warner Music Sweden AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Warner Music Sweden AB (Warner Music) (556055-2605) has processed personal data in breach of Article 6 and 7.3 of the General Data Protection Regulation (GDPR)¹ by not providing sufficient information about the right to withdraw consent.

IMY issues a reprimand to Warner Music pursuant to Article 58(2)(b) of the GDPR.

Presentation of the supervisory case

IMY has initiated supervision regarding Warner Music due to a complaint. The complaint is one of several complaints submitted to the European Data Protection Authorities regarding cookies and cookie banners. The complaints mainly concern the design of cookie banners, the placement of cookies and the subsequent processing of personal data after the cookies have been placed on the complainant's browser or device. To facilitate the cooperation on these complaints, a 'Cookie Banner Taskforce' was created within the European Data Protection Board.

In view of the cross-border nature of the processing, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Austria and Italy.

The complainant has essentially stated the following. On 21 May 2021, Warner Music processed the complainant's personal data in breach of the GDPR because there was no valid consent. Warner Music has not had a prominent option to withdraw the consent in the same way as there is to give the consent. Not having an option to withdraw that is as easy to find as the cookie banner, makes it not as easy to withdraw

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

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).

consent as to give it. Warner Music's information about the use of cookies on the website (in a so-called cookie banner) has been attached to the complaint.

Warner Music has essentially stated the following. The legal basis for the subsequent processing of personal data collected through the setting of cookies is consent. The company fulfils the conditions for consent described in Article 7 of the GDPR, *inter alia*, by means of the information provided in the company's cookie banner on its website. The cookie banner contains information about the use of cookies and information about the processing of personal data collected through the setting of cookies. Visitors to the website can make clear choices through the cookie banner to enable an informed and voluntary choice regarding the processing of personal data. Visitors are also informed through the cookie banner that they have the choice to withdraw their consent at any time. The cookie banner shows that the visitor can manage their options for cookies on the company's website by clicking on 'cookie settings'. This link appears on all pages of the website.

Warner Music has further proposed changes to its cookie banner, to include the wording 'you can withdraw your consent at any time'. The updates would include the wording in both the first and second layers of the banner.

Definition of the case

The Swedish Post and Telecom Authority is the sole competent supervisory authority over the Electronic Communications Act (2022:482), which lays down specific requirements for the storage of cookies in terminal equipment or the collection of data from such equipment. However, the personal data processing that takes place after collection, such as analysis or profiling, is subject to the rules of the General Data Protection Regulation, where IMY is the competent supervisory authority. Against that background, IMY's examination has been limited to the processing of personal data that took place after the data was collected and the deficiencies alleged in the complaint relating to that subsequent processing.

Motivation for the decision

Applicable provisions, etc.

Processing of personal data is only lawful if one of the conditions set out in Article 6 of the GDPR is met. The legal basis in question in the case is consent pursuant to Article 6(1)(a).

Consent is defined in Article 4(11) of the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. For consent to be valid, all of these requirements must be met.

The transparency of the processing of personal data regarding the data subject is set out in Article 5(1) of the Regulation. It is in the light of that principle that the requirement that consent must be informed must be read.

Article 7(3) of the GDPR provides that, in order for consent to be valid, the data subject must have the right to withdraw his or her consent at any time. Before consent is

given, the data subject shall be informed thereof. It should be as easy to withdraw as it is to give consent.

The recitals to the GDPR state that natural persons should be made aware, inter alia, of their rights in relation to the processing of personal data and of how to exercise their rights in relation to the processing.²

The European Data Protection Board (EDPB) guidelines on consent state that giving and withdrawing consent must not always be done through the same action, but should be as simple. In practice, when consent is given electronically by a single mouse click, swipe or keystroke, data subjects must be able to withdraw consent just as easily. Where consent is obtained through a service-specific user interface (e.g. via a website or an app), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw the consent without difficulty. This means, among other things, that a controller must ensure that it does not cost anything to withdraw consent and that lowering the service level.³

The EDPB further considers that information on the right to withdraw consent is a minimum requirement for the consent to be considered informed, and thus to be a valid consent. This information must be provided before the user gives his or her consent. Providing information on the possibility of withdrawal is necessary for the user to exercise his or her right to withdraw his or her consent. If the controller does not provide easily accessible information, the user's consent becomes an invalid ground for processing.⁴ When requesting consent, controllers should ensure that they always use clear and plain language. For example, the declaration of consent must be names as such. Phrases like 'I know that...' does not meet the requirement of clear language.⁵

The issue in the case is if there has been a valid consent in order to processing the complainant's personal data through the use of cookies.

Assessment

Warner Music provides information that cookies are used on the website in a so-called cookie banner that is displayed, among other things, when the user first enters the website. In the first layer of the cookie banner, as it appeared at the time of the complaint, there are three equally prominent choices: 'Cookie settings', 'Reject all' and 'Accept all cookies'. The following assessment is based on this cookie banner and the company's website.

Clear and unambiguous information on the right of withdrawal

IMY considers that the controller must provide information on the possibility of withdrawing consent in order to comply with the informed consent requirement. Withdrawal of consent is a right that every data subject has when consent has been used as a legal basis. It is therefore necessary that a user receives this information before consent is given. The EDPB Guidelines state that a controller should always use clear and plain language when requesting consent. IMY considers that the

² Recital 39.

³ EDPB Guidelines 05/2020 on consent under Regulation (EU) 2016/679, version 1.1, adopted on 4 May 2020, paragraphs 113-114. Swedish version.

⁴ A.a. paragraphs 62-64 and 116.

⁵ A.a. paragraph 67.

requirement for clear and plain language should also apply to information on withdrawal of consent. This means that it must be clear to the complainant that he or she has the right to withdraw his or her consent.

Neither the information text on the cookie banner nor the website in general says anything about a user's right to withdraw their consent at any time. Instead, the information text in the cookie banner states that 'You can manage your cookie choices on our site now or later by clicking on 'Cookie settings'. 'Cookie settings' indicates 'Update your cookie settings at any time by clicking on 'Cookie settings' on all pages, which will then take you back to this settings centre'.

Simply providing information about the possibility of administering their cookie choices or updating settings is not sufficient to make it clear to a user that there is a right to withdraw consent.

In the light of Article 7(3) of the GDPR, recital 39 and the EDPB Guidelines on Consent, IMY considers that Warner Music did not inform the complainant on the right to withdraw a consent in a sufficiently clear manner to enable him or her to defend his or her rights. Therefore, the complainant cannot be considered to have given an informed consent. As there was no information on the right to withdraw, it has not been as easy to withdraw as to consent.

Comparison of consent and withdrawal procedures

The complainant highlights the option of having a permanently hovering icon visible on all pages of the website to withdraw consent. IMY believes that a permanent hovering icon is an option that can meet the condition that it should be as easy to withdraw as to give consent. On the other hand, IMY does not consider that the GDPR requires a specific technical solution that all controllers must use in order to comply with the requirement of Article 7(3). The assessment of whether it is as easy to withdraw as it is to give consent needs to be made in the individual case on the basis of the procedure in question used to give consent. This assessment is in line with the Cookie Banner taskforce report and the EDPB opinion on valid consent.⁶

At the relevant time, when a user first visited Warner Music's website, the cookie banner appeared immediately. There, the user could, at the click of a button, consent to the use of all (non-essential) cookies. Once a user had given their consent in the cookie banner, the cookie banner disappeared. In order to withdraw the consent, the data subject had to click on the 'cookie settings' link located at the bottom of the footer. When you clicked on the link, you ended up in a settings center, in the second layer of the view. In the settings centre, the data subject had to uncheck the categories of the cookies to which he or she had previously consented, and then confirm his or her choices. When comparing the way consent was obtained on the website, fewer keystrokes were needed to give consent than to withdraw consent.

Since the relevant period, Warner Music has changed its settings centre to which the data subject accesses after clicking on 'cookie settings'. The data subject no longer has to uncheck the categories of cookies to which he or she has consented, but can choose directly to 'reject all'. IMY considers that this measure facilitated the withdrawal of consent by the data subject. As a result of this improvement, IMY considers that the deficiency that existed at the time of the complaint, in this respect, no longer persists.

⁶ Report on the work of the Cookie Banner Taskforce, adopted on 17 January 2023, para. 35 and Opinion 08/2024 on valid consents for "Consent or Pay Models" implemented by large online platforms, adopted on 17 April 2024, paragraph 169 (IMY translation).

The "cookie settings" link is permanently available on all pages of the website and the data subject can withdraw his or her consent with one keystroke after pressing the link. IMY's assessment is therefore that this deficiency has been remedied.

Summary

Warner Music has not provided sufficiently clear information about the possibility of withdrawing consent and the data subject has thus not been able to give informed consent. Since there was no information about the right to withdraw, it has not been as easy to withdraw as to consent on the company's website warnermusic.se. There was therefore no valid consent and therefore no legal basis for processing the complainant's personal data. Warner Music therefore processed the complainant's personal data in breach of Article 6 and Article 7(3) of the GDPR.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case need to be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. IMY has assessed that the company has not had a legal basis to process the complainants' personal data. Although Warner Music is not considered to have made the withdrawal as easy as the giving of consent, there has been an opportunity to withdraw the consent via a permanently accessible link on the website. Warner Music has provided some information that the data subject may change their choices, even if this is considered insufficient. Warner Music has also made some improvements, after receiving the complaint, to make it easier for data subjects to withdraw consent. The company has not previously been found to have infringed the General Data Protection Regulation.

Since Warner Music has also stated that it intends to add clear and precise information on the right to withdraw consent to its cookie banner, IMY does not consider it appropriate to order it to do so.

Against this background, IMY considers this a minor infringement within the meaning of recital 148 and that Warner Music is to be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

Swedish ref. no.
DI-2021-10063

IMI case register:
164557

Date:
2024-11-16

Final decision pursuant to Article 60 under the General Data Protection Regulation – Klarna Bank AB

Decision of the Privacy Protection Authority

The Swedish Data Protection Authority (IMY) finds that Klarna Bank AB (556737-0431) has processed the complainant's personal data in breach of Article 12(3) of the General Data Protection Regulation¹ (GDPR) by failing to provide the complainant access to their personal data without undue delay.

IMY issues a reprimand to Klarna Bank AB pursuant to Article 58(2)(b) of the GDPR for the breach of Article 12(3).

Presentation of the supervisory case

Proceedings

The Privacy Protection Authority has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint dated 20 March 2020. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complaint has been lodged (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The supervision has been initiated in order to investigate whether the complainant's request for access has been properly received and handled (Article 15 GDPR), whether the complainant's request for erasure has been properly received and handled (Article 17 GDPR) and whether the complainant's requests for access and erasure have been handled within the statutory time limits (Article 12 GDPR).

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Germany, Denmark, Austria, Italy, Poland and Finland.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

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).

The complaint

The complainant has primarily stated that on 20 December 2019, he unsuccessfully requested access to and erasure of his personal data. Klarna has instead on 5 February 2020 referred him to submit his request for deletion to datenschutz@klarna.de and referred to their application for further information. The complainant contacted Klarna on 6 February 2020 stating that he had not been able to find the information he was looking for and reiterating his request for access. The complainant also sent a reminder to Klarna on 8 March 2020. Despite repeated contact with Klarna, the company has not complied with his requests for access and deletion.

What Klarna has stated

Klarna has essentially stated the following. Klarna's dispute resolution team contacted the complainant by email on 20 December 2019 regarding an order paid by the complainant with Klarna where the complainant received faulty goods. On the same day, the complainant replied to the abovementioned email concerning the dispute and, in the same email, submitted requests for access and for erasure. Due to a large number of cases, Klarna initially missed that the complainant's message also contained a request for access or deletion. As soon as Klarna discovered this, they contacted the complainant on 5 February 2020 and referred him to submit his request for access and deletion respectively to datenschutz@klarna.de.

The complainant never returned any request to datenschutz@klarna.de. Instead, the complainant contacted Klarna's dispute resolution team and later also their customer service to remind them of his request. Klarna then initiated a process to verify the identity of the complainant. As they did not have all the necessary identification points according to the procedure in place at the time, it took until 9 August 2023 for them to be able to comply with the complainant's request for access. The complainant had then informed Klarna that he would wait until further notice to delete his data.

Klarna notes a posteriori that, at the time of the first contact on 20 December 2019, the complainant could have been identified with the information provided by the complainant at that time, with the proviso that the email address used by the complainant at the time of the purchase should have been confirmed first.

Since the time of the complainant's first contact, Klarna has been working on improving their processes to ensure rights under the GDPR. Among other things, the company has reduced its processing times and now handles requests for access regardless of the channel through which it has been received. The company has also updated its identification routine so that e-mail confirmations are no longer needed when Klarna can confirm that the e-mail address that the complainant contacted Klarna via is the same as used for purchases by the complainant.

Communication in the case

IMY has communicated Klarna's reply to the relevant national supervisory authority in the country where the complainant lodged the complaint. The German data protection authority has indicated that the complainant did not wish to comment on the response of the supervised entity due to the lengthy processing time.

Reasons for the decision

Applicable provisions, etc.

It follows from Article 15 of the GDPR that the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, if so, access to the personal data and certain specified information.

It follows from Article 17 of the GDPR that the controller is obliged to delete personal data without undue delay if one of the conditions set out in that article is met.

According to Article 12(3): Upon request, the controller shall, without undue delay and in any event no later than one month after receiving the request, provide the data subject with information on the measures taken pursuant to Articles 15 to 22. That period may be extended, if necessary, by a further two months, taking into account the complexity of the request and the number of requests received. The controller shall notify the data subject of such an extension within one month of receipt of the request, stating the reasons for the delay.

The European Data Protection Board (EDPB) Guidelines 01/2022 on access state that the calculation of the one-month deadline in Article 12(3) is calculated from the date of receipt of the request. Where, upon receipt of the request, the controller needs to take measures to ensure the identity of the data subject, the time limit may be suspended until the controller has received the information necessary to identify the data subject. provided that the request for additional information has been made without undue delay. The guidelines further state that if a data subject makes a request using a communication channel provided by the controller, the controller must handle such a request, even if the controller prefers another channel.²

IMY's assessment

Right of access

IMY notes that the GDPR does not lay down any formal requirements as to how a request for access under Article 15 is to be made and that there are therefore, in principle, no requirements under the GDPR that data subjects must observe when choosing the communication channel they use to contact the controller. In this case, the data subject has contacted Klarna directly with a clear request for access on 20 December 2019. Klarna only discovered the complainant's request on 5 February 2020. IMY considers that the action taken by Klarna at that time, referring the complainant to their email address datenschutz@klarna.de, was not sufficient to satisfy the complainant's request. Furthermore, the measure was not taken within the time frame laid down by the GDPR.

Furthermore, the investigation shows that Klarna did not respond to the complainant's request for access until 9 August 2023. It does not appear that the complainant's request was particularly complex. Klarna also stated that, at the time of their first contact on 20 December 2019, they had sufficient information to verify the

² European Data Protection Board (EDPB) Guidelines on the right of access - Guidelines 01/2022 on data subject rights – Right of access, version 2.0, adopted on 28 March 2023, paragraphs 52-53 and 159.

complainant's identity. IMY therefore finds no reason to extend the time limit of one month in Article 12(3).

In an overall assessment, IMY considers that Klarna has processed the complainant's personal data in breach of Article 12(3) by not giving the complainant access to his personal data without undue delay.

Right to erasure

From the information provided by Klarna, it appears that the complainant no longer asserts his request for erasure. The complainant has been given the opportunity to comment on what Klarna has put forward but has refrained from commenting on the information. IMY therefore considers that there is no deficiency under Article 17 of the GDPR.

Choice of intervention

IMY has found above that Klarna has failed to fulfil their obligations under Article 12(3) of the GDPR. The last question to be considered by IMY is what action should be taken in response to the infringement.

In the event of infringements of the GDPR, IMY has a number of corrective powers, including reprimands, injunctions and fines. It follows from Article 58(2)(a) to (j) of the GDPR. According to recital 129 of the GDPR, IMY must take such measures as are appropriate, necessary and proportionate to ensure compliance with the GDPR.

According to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case need to be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The investigation is based on an individual complaint and concerns shortcomings in the processing of data relating to an individual data subject. There has been no question of the processing of sensitive personal data. The prescribed time limit of a maximum of one month has been exceeded by more than 3 years and 7 months. However, the complainant's right of access has been granted. The deficiency in question is therefore of a less serious nature than if the request had been left unanswered. The investigation shows, among other things, that the company has updated its procedures for handling requests for access and now handles the request regardless of the channel through which the request was received, that the company has reduced its processing time for incoming cases and that the company has reviewed its identification routine and made it clearer and more efficient.

Against this background, IMY considers this a minor infringement within the meaning of recital 148 of the GDPR. In the light of the foregoing, IMY considers that a

reprimand is an appropriate, necessary and proportionate measure for the infringements at issue. The company must therefore be granted a reprimand pursuant to Article 58(2)(b) of the GDPR.

This draft decision has been approved by the decision-maker [REDACTED] after a presentation by the legal advisor [REDACTED].

Annex

Complainant's personal data

Copy to

Data Protection Officer: [REDACTED]

Complainant

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

COMPLAINANT

See appendix

TILLSYNSOBJEKT

CDON AB

Diarienummer:
IMY-2023-16164

Nationell ref:627/154/21

Final decision under the General Data Protection Regulation – CDON AB

IMI case register:
580527**Datum:**
2024-11-14

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that CDON AB 556406-1702 has processed personal data in breach of Article 17 of the General Data Protection Regulation (GDPR)¹ by failing to comply with the complainant's request for erasure.

Pursuant to Article 58(2)(c) of the GDPR, IMY orders CDON AB to comply with the complainant's request to exercise its right to erasure under Article 17 of the GDPR. This is done by erasing, subject to any applicable exceptions in Article 17(3) of the GDPR, all personal data that CDON AB processes about the complainant and informing the complainant of these measures in accordance with Article 12(3). The measures shall be implemented no later than two weeks after this decision has become final.

The case is closed.

Presentation of the supervisory case

IMY has initiated supervision regarding CDON AB (CDON AB) due to a complaint. The complaint has been submitted to IMY as the lead supervisory authority under Article 56 GDPR. The handover has been made from the supervisory authority of the country where the complainant lodged his complaint (Finland) in accordance with the Regulation's provisions on cooperation in cross-border processing.

Since it is a cross-border complaint, IMY has used the mechanisms for cooperation and consistency in the GDPR. The concerned supervisory authorities have been the data protection authorities of Finland, Denmark, Norway and Italy.

The complainant essentially states the following: The complainant requested erasure according to article 17 GDPR from CDON AB on January 18th 2021. The complainant received an email from CDON AB on January 20th 2021 asking the complainant for more information to be able to comply with the request.

CDON AB essentially states the following. CDON AB is the controller for the processing of personal data to which the complaint relates. The complainant submitted

Postadress:
Box 8114
104 20 Stockholm**Webbplats:**
www.imy.se**E-post:**
imy@imy.se**Telefon:**
08-657 61 00

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).

his request for erasure on January 18th 2021 by email. The request has not been met because the complainant did not reply to the security questions asked by CDON AB in order to verify and identify the complainant. The questions are asked in order to ensure that the person who requested erasure is the correct data subject. Since the identity of the complainant could not be verified, CDON AB considered themselves to be prevented from complying with the request of erasure, as it would be in breach of the requirements of appropriate technical and organisational security (Article 32 GDPR). CDON AB only requested answers to two of the questions asked, in order to verify the data against the data already processed about the data subject. CDON AB always strives to minimise the risk of handling data subjects' personal data due to the possibility of false requests. Against this background, CDON AB has not been able to meet the complainant's request for erasure.

CDON AB further states that CDON AB was unable to assess whether the person who contacted them was actually the person they claimed to be. In those circumstances, CDON AB considered that they had reasonable grounds to doubt the complainant's identity at that time. CDON AB considered that the gravity of the consequences would be significant if the wrong individual's personal data were to be erased, as well as if the personal data were to be erased at the request of the wrong party. The answers to the questions asked by CDON AB were about data that was already available to CDON AB because the data subject provided it when creating a user account and when they completed payment for their last order.

IMY has sent CDON AB's statement to the supervisory authority of the country where the complainant lodged their complaint (Finland) to give the complainant opportunity to comment on CDON AB's statement. The complainant has not responded.

Motivation for the decision

Furthermore, it follows from Article 5(2) that the controller must be responsible for and be able to demonstrate compliance with the principles listed in Article 5(1) ('accountability').

Article 24 of the GDPR regulates the liability of the controller. The article states that, taking into account the nature, scope, context and purposes of processing and the risks, of varying likelihood and severity, to the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is carried out in accordance with this Regulation.

According to Article 17(1) GDPR, the data subject shall have the right to obtain from the controller the erasure of his or her personal data without undue delay and the controller shall be obliged to erase personal data without undue delay, under certain conditions set out in the relevant article.

The controller may, where it has reasonable doubts as to the identity of the natural person making the request pursuant to Article 17, request the provision of additional information necessary to confirm the identity of the data subject. This follows from Article 12(6) of the GDPR.

CDON AB has described its procedures for identifying data subjects, but has not provided any explanation of concrete circumstances as to why CDON AB had reason to doubt the identity of the complainant. IMY finds that no other evidence has been

found to show that CDON AB had reason to doubt the identity of the complainant. Against this background, IMY considers that CDON AB had no reason to doubt the identity of the complainant. CDON AB has thus not shown that they were justified in refusing to comply with the complainants request. IMY therefore finds that CDON AB has failed to comply with Article 17 of the GDPR.

Pursuant to Article 58(2)(c) of the GDPR, IMY orders CDON AB to comply with the complainant's request to exercise its right to erasure under Article 17 of the GDPR. This is done by erasing, subject to any applicable exceptions in Article 17(3) of the GDPR, all personal data that CDON AB processes about the complainant and informing the complainant of these measures in accordance with Article 12(3). The measures shall be implemented no later than two weeks after this decision has become final.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

Appendix

The complainant's personal data

COMPLAINANT

See appendix

CONTROLLER

Klarna Bank AB

Swedish ref.:
IMY-2022-10759

DE SA ref.:
521.15494

IMI case register:
164557

Date:
2024-11-12

Decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection

The case is closed.

Presentation of the supervisory case

IMY has initiated supervision regarding Klarna Bank AB (Klarna) in order to investigate whether Klarna has handled the complainant's request of access in accordance with articles 15 and 12.3 in the General Data Protection Regulation. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complaint has been lodged (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Germany, Denmark, Austria, Italy, Poland and Finland.

The German supervisory authority has stated that the complaint has been withdrawn.

Motivation for the decision

IMY shall handle complaints about incorrect processing of personal data and, to the extent appropriate, investigate the subject matter of the complaint (Article 57(1)(f) GDPR).

The complaint has been withdrawn. Therefore, IMY finds no reason to take any further action in the case. The case is closed.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

This decision has been made by decision maker [REDACTED] after presentation by legal advisor [REDACTED].

Appendix

The complainant's personal data

Copy to:

DPO, Klarna Bank Ab

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.

Mag Interactive AB
Organisation number 556804-3524
Drottninggatan 95A
113 60 Stockholm

Our ref.:
DI-2020-10538, IMI no. 120399

Date:
2021-01-22

Supervision under the General Data Protection Regulation - Mag Interactive AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that MAG Interactive AB has processed personal data in violation of Article 12.3 of the GDPR¹ by not informing the complainant without undue delay of the result of the complainant's request of 29 May 2019 for erasure pursuant to Article 17 no earlier than 6 November 2020.

The case is closed without further action.

Description of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding MAG Interactive AB (the company) due to a complaint. The complaint has been transferred to IMY, as lead supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR), from the supervisory authority of the country where the complainant has lodged the complaint (Austria), in accordance with the Regulation's provisions on cooperation in cross-border matters.

The complaint states that the company has not handled the complainant's request for erasure of the complainant's personal data pursuant to Article 17 of the GDPR.

Mag Interactive AB has mainly stated the following. The company first received a request for erasure of the complainant's account on the company's services on 29 November 2018 (the first request). Since the request came from an e-mail address other than the one linked to the account, the company requested that the complainant return with proof of their identity, which the complainant did not. On 29 May 2019, a new request for deletion of the complainant's account was received, but then by post and with the necessary evidence to confirm the complainant's identity (the second request). The company deleted the complainant's data manually in accordance with the request of 15 June 2019, except for the information needed to show that the request had been handled. However, due to an oversight, the complaint was not informed of the outcome of the request in connection with the request being handled.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

¹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Instead, it was only discovered and done in connection with the review pursuant to this supervisory matter, i.e., on 6 November 2020.

The investigation has been carried out in written form. In light of it being a cross-border complaint, the Swedish Data Protection Authority has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Ireland, Norway, France, Austria, Denmark, Poland and Germany.

Justification of the decision

Applicable provisions

According to Article 12(3) of the GDPR, the controller shall, upon request, without undue delay and, in all circumstances, at the latest one month after receiving the request, provide the data subject with information on the measures taken pursuant to Article 17. If necessary, this period may be extended by an additional two months, taking into account the complexity of the request and the number of requests received. The controller shall notify the data subject of such an extension within one month of receipt of the request and indicate the reasons for the delay.

According to Article 12(6), the controller may, if he or she has reasonable reason to doubt the identity of the natural person who submits a request pursuant to Article 17, that additional information necessary to confirm the identity of the data subject may be provided.

According to Article 17.1 a, the data subject shall have the right to have their personal data erased by the controller without undue delay and the controller shall be obliged to erase personal data without undue delay if the personal data is no longer necessary for the purposes for which they were collected or otherwise processed. According to Article 17(3)(b), this shall not apply to the extent that the processing is necessary to fulfil a legal obligation requiring processing under Union law.

According to Article 57(1)(f), each supervisory authority on its territory shall be responsible for the processing of complaints from a data subject and where appropriate to investigate the matter of the complaint.

The Swedish Authority for Privacy Protection's assessment

Regarding the first request, IMY finds that MAG Interactive AB had reasonable reason to doubt the identity of the complainant and thus request that the complainant submit additional such evidence, which the complainant did not respond to. Against this background, IMY considers that the company was not obligated to take any further measures due to the request.

Regarding the second request, IMY notes that the Company has deleted the complainant's information, except the information required to show that the request has been processed, within 16 days of the company receiving the request on 29 May 2019. IMY finds that the company has erased the complainant's information without undue delay in the sense referred to in Article 17 of the GDPR and has had the right to retain the information needed to demonstrate that the request has been handled in accordance with the GDPR.

On the other hand, the company informed the complainant of the result of the second request only on 6 November 2020. Since the controller shall, pursuant to Article 12(3) without undue delay and, in any event, no later than one month after receiving the request, with an exemption not relevant here, inform the data subject of the measures taken pursuant to Article 17, MAG Interactive AB has thereby infringed that article.

The company has stated that the reason why the complainant was not informed if the result of the request was due to an oversight. According to the company, this was mainly due to the request being handled manually because it was received by mail and that the company normally handles requests in a system where notifications on measures taken are sent automatically. As a result of the incident, the company has indicated that it will review its procedures so that it does not happen again. This includes setting up a separate log for manual cases so that it can be ensured that all steps are followed and that the user is notified as requested.

IMY notes that it is of course important that controllers inform data subjects of what measures have been taken in connection with the request, even in cases where the request is fully met to the extent required.

However, in light of the circumstances regarding the infringement that the company has highlighted – and the measures stated by the company that it has taken and will take – IMY considers that the subject matter in the complaint has been investigated to the extent appropriate under Article 57(1)(f) of the GDPR.

Against this background, the matter is concluded without further action.

This decision has been made by Unit Manager [REDACTED] after presentation by legal advisor [REDACTED].

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protections (IMY) decision 2021-01-22, no. DI-2020-10538. Only the Swedish version of the decision is deemed authentic.

Klarna Bank AB
Sveavägen 46
111 34 Stockholm dataprotectionofficer@klarna.com

Our ref:
DI-2020-10546, IMI no.155160

Date:
2021-01-25

Final decision in IMI case reg no 155160 – Supervision under the GDPR against Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The case will be written off from further investigation.

Description of the supervisory case

The Swedish Authority for Data Protection (the Swedish SA) has initiated an investigation against Klarna Bank AB (the company) due to a complaint. The complaint has been submitted to the Swedish SA, in its capacity as lead supervisory authority for the company's operations pursuant to Article 56 of the GDPR, from the supervisory authority in the country where the complainant has lodged the complaint in accordance with the Regulation's provisions on cooperation in cross-border matters.

The complainant stated that the company has sent direct marketing e-mails to him despite having objected to processing of personal data for direct marketing purposes. Furthermore, the complainant has argued that he has not received information that his personal data will be processed for direct marketing purposes and that he has not given his consent to such processing of personal data.

Klarna Bank AB has essentially stated the following. The company is not the controller for the processing concerned in this complaint. The company does not know who is behind these mailings and are not able to further investigate the matter based on the screenshots attached to the complaint. According to the company, the e-mails that form the basis of the complaint constitute so-called spam. The company has previously received notice of e-mails sent from the address noreply-no@klarna.no. The company then initiated an internal investigation and concluded that these e-mails constituted spam. The company believes that the approach for sending these emails is spoofing, i.e. the sender tries to imitate or mimic Klarna as the sender. The company states that they cannot prevent or affect these mailings as the company is not involved in the processing in question. Furthermore, the company adds that they have previously informed their customers about spam emails from noreply-no@klarna.no by temporarily publishing a banner on their website.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

In light of the complaint involving cross-border processing, the Swedish SA has used the mechanisms for cooperation and consistency contained in Chapter VII of the

GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, Denmark, Finland, Germany, Belgium, Italy and Spain.

Justification of the decision

Applicable provisions

Article 4(1) of the GDPR defines the concept of personal data as any information relating to an identified or identifiable natural person.

Article 4.2 states that processing refers to any operation or set of operations which is performed on personal data or on sets of personal data.

According to Article 4.7, the controller entails a natural or legal person, public authority, agency or other body that alone or jointly with others determines the purposes and means of the processing personal data.

The Swedish Authority for Privacy Protection's assessment

The Swedish SA constituted that processing of personal data has taken place by the emails sent with direct marketing to the complainant's e-mail address. However, the company had put forward that they are not the controller responsible for the processing of personal data that has taken place. There has been no reason to question the company's information. The case will thus be written off from further investigation.

This decision has been taken by Head of Unit [REDACTED] after presentation by legal adviser [REDACTED]

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protections (IMY) decision 2021-01-25, no. DI-2020-10546. Only the Swedish version of the decision is deemed authentic.

Our ref.:
DI-2020-10518, IMI case no
134712

Date:
2021-03-31

Supervision under the General Data Protection Regulation – Klarna Bank AB

Final decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Klarna Bank AB has violated Article 12(3) GDPR¹ by

- regarding complaint 1: not without undue delay respond to a request of access pursuant to article 15.

The Swedish Authority for Privacy Protection gives Klarna Bank AB a reprimand in accordance with Article 58(2)(b) of the General Data Protection Regulation.

Description of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (the company) due to two complaints. Each complaints have been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation, from the supervisory authority of the country where the complainants have lodged their complaint (Austria and Germany) in accordance with the Regulation's provisions on cooperation in cross-border matters.

The complainants have stated that they have requested access to their personal data in accordance with Article 15 of the General Data Protection Regulation. Due to the complaints, IMY has initiated supervision to investigate whether the complainants' requests for access under Article 15 have been met and whether it has been made within the specified time limit in Article 12(3).

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

Klarna Bank AB states that they are the controller for the processing of personal data that the complaints concern. The company also states that they handle a large amount GDPR related requests.

¹Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Complaint 1 (from Austria with national reference number: D130.247)

Regarding the first complaint, the company states that the complainant's request for access was received by the company via e-mail on 5, 10 and 29 January 2019. Since the request was received to a different email address than the one referred to by the company for data protection issues, the request was not processed in accordance with the company's internal processing procedures. This led to a longer processing time and that information and a copy of the complainant's personal data according to Article 15 were not sent until 18 June 2019. The company also states that they have promptly answered the complainant's follow-up questions regarding the company's personal data processing, which the complainant has been satisfied with.

Complain 2 (from Germany with national reference number: LDA-1085.1-13373/19-F)

Regarding the second complaint, the company states that the complainant's request for access was received to the company's chat on 28 October 2019. The complainant repeated their request by e-mail on 30 October 2019. The company contacted the complainant on 6 November 2019 to request additional information. These were provided the same day. On 11 November 2019 the company sent out information and a copy of the personal data to the complainant pursuant to Article 15, i.e. within 14 days of receiving the request. On 14 November 2019, the company sent more detailed information about the company's automated decision-making on purchases. The complainant contacted the company again on 13 December 2019 due to the fact that they had not received the company's mailings. The company requested a new address on 7 January 2020 and has not received a reply.

The investigation has been carried out in written form. In light of it being two cross-border complaints, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the General Data Protection Regulation. The supervisory authorities concerned have been the data protection authorities in Austria, Germany, the Czech Republic, Denmark and Norway.

Justification of decisions

Applicable provisions

To anyone who requests a data controller is obliged to provide information about whether or not their personal data is being processed. If such data is processed, the controller shall, in accordance with Article 15 of the General Data Protection Regulation, provide the applicant with supplementary information and a copy of the personal data processed by the controller.

According to Article 12(3), a request for access must be handled without undue delay and in any event no later than one month after the request has been received. The time limit of one month may be extended by an additional two months if the request is particularly complicated or the number of requests received is high.

If the period of one month is extended, the controller must notify the data subject of the extension. The notification of the extension of the time limit shall take place within one month of receipt of the request. The controller must also specify the reasons for the delay.

According to Article 12(6), the controller may request, if he or she has reasonable reason to doubt the identity of the natural person who submits a request pursuant to Article 15, that additional information necessary to confirm the identity of the data subject may be provided.

The Swedish Authority for Privacy Protection's assessment

Has there been an infringement of the GDPR?

Complaint 1 (from Austria with national reference number: D130.247)

Regarding the first complaint IMY states that the complainant has been provided with information and a copy of the personal data being processed pursuant to Article 15 of the General Data Protection Regulation. However, the right to access was only granted after more than five months from the date the first request was submitted. The request has therefore not been handled without undue delay and within the stipulated time limit in Article 12(3). The complainant has also not been informed of the delay.

What the company has stated about handling a large number of requests under the General Data Protection Regulation and the fact that follow up questions have been answered quickly does not lead to any other assessment concerning the delay and thus the infringement of article 12(3) in one case.

Complaint 2 (from Germany with national reference number: LDA-1085.1-13373/19-F)

Regarding the second complaint IMY states that the complainant has been provided with information and a copy of the personal data pursuant to Article 15. The information was provided without undue delay. After the complainant pointed out that they had not received the mailing, the company requested alternative contact details. Against this background, IMY considers that the company has not been obliged to take any further action on the basis of that request.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) the IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines may be imposed in addition to or instead of the other measures referred to in Article 58(2). Furthermore, Article 83(2) states which factors should be taken into account in decisions on whether administrative fines should be imposed and when determining the amount of the fine. In case of a minor infringement, IMY may, as stated in Recital 148, instead of imposing a sanction fee, issue a reprimand pursuant to Article 58(2)(b). In this assessment, regard shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous infringement of relevance.

In an overall assessment of the circumstances IMY considers that it is a matter of a minor infringement, regarding complaint 1, and that Klarna Bank AB should therefore be given a reprimand pursuant to Article 58(2)(b) for the stated infringement.

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-03-31, no. DI-2020-10518. Only the Swedish version of the decision is deemed authentic.

Spotify AB
Org. no:556703-7485
Regeringsgatan 19
111 53 Stockholm

Our ref.:
DI-2020-10541, IMI no. 75661

Date:
2021-03-24

Supervision under the General Data Protection Regulation – Spotify AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Spotify AB has processed personal data in violation of

- Article 12(4) of the General Data Protection Regulation (GDPR)¹ by in its reply of 8 June 2018 to the complainant's objection to the processing pursuant to Article 21 of 24 May 2018 having not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer has not contained information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The Swedish Authority for Privacy Protection (IMY) issues Spotify AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Report on the supervisory matter

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Spotify AB (the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Denmark) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The *complaint* is essentially the following. The complaint has previously had an account and a payment subscription to the company's music service. The complainant has several times requested that the company erase his card details. According to the company, the complainant has registered via PayPal and the company therefore does not process the complainant's card details. The complainant questions this because the complainant's son has been refused to register for a free trial period where the

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

¹Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

complainant's card information has been used, on the grounds that the card has already been used.

Spotify AB has mainly stated the following.

The complainant has requested deletion of his credit or debit card information. However, Spotify does not process card data when a user pays via PayPal, such as the complainant, but instead treats unique identifiers for the payment cards or "instruments" ("unique payment instrument identifiers") used by a customer when registering free trial periods. The legal basis for the processing is legitimate interests. That the complainant has written that he withdraws his consent may be interpreted as an objection to the processing. The continued processing is not subject to the right to erasure because Spotify has a strong, legitimate interest in continuing the processing that outweighs the rights and freedoms of the complainant.

To register for a free trial, potential customers must provide Spotify debit card details that will be used for invoicing once the free trial has expired. To counter the abuse of the free trials offered by the company, the company uses unique payment instrument identifiers. This means that the same payment instruments cannot be used several times. Without this feature, it would be easy for a customer to start new free Spotify accounts for additional trials each time their free trial expires, by varying tasks such as email address, and thus fraudulently exploiting Spotify. The unique payment instrument identifier is an alphanumeric chain generated by Spotify payment processor PayPal. It allows for the unique identification of credit cards, but it does not contain the credit card number or other card details. Spotify cannot, through the payment instrument identifier, access to debit card information via reverse engineering. This process is compatible with PCI DSS².

The processing is necessary for Spotify in order to counteract fraud. This is both a legitimate interest in Spotify and the company's broad customer base, as the company could not continue to offer free trials of the company's service if fraud could not be counteracted in this way. It is also in the public's legitimate interest.

Spotify has responded to the complainant's request but has not deleted the data because the right to erasure is not applicable. The company responded on 7 December 2017 to the complainant's original request of 6 December 2017 and 8 June 2018 to the complainant's most recent request of 24 May 2018 and thus within the deadline of the GDPR. Regarding the complainant's letter of 15 March 2018, the company did not interpret it as a request for deletion under the GDPR, but responded to the letter on 4 May 2018. In several of these answers, the company has informed the complainants that the Company does not store his debit card information and that the company could not erase the payment instrument reference that identifies that his card has already been used to access one of the company's offers or services.

Regarding the information provided to the complainant on 8 June 2018 due to his objection, Spotify believes that the company responded to the complainant's question by explaining that it does not store any card information but only uses an algorithm to see if a credit card has been used to access a Spotify offer earlier. If the company had had reason to believe that the complainant wanted more details about these categories of personal data, the company would have provided it. When the company's customer service advisors communicate with users, the company always

²PCI DSS stands for Payment Card Industry Data Security Standard and is a widely accepted set of guidelines and procedures aimed at optimising security around the use of credit and debit cards.

tries to provide the information that users ask for in a format that is relevant to the users and which also someone who does not know the provisions of the GDPR would understand. Since the complainant neither mentioned the regulation nor asked for the legal basis for the processing, the company did not address legal details in its response such as the company's balance of interests. In addition, in its privacy policy, the company had communicated to its users that it would like to provide more information on the weighing of interests that the Company has made to rely on legitimate interest as a legal basis and informed of the possibility of filing a complaint with the supervisory authorities. It should also be taken into account that the matter was started more than five months before the GDPR came into force and that the only correspondence that took place in the time after was the company's response two weeks thereafter. Since then, the company's customer service advisors have undergone further training on how to answer users in a clear and clear manner, which questions should be regarded as inquiries under the GDPR and what questions should be forwarded to the company's data protection team and data protection officer. Finally, it must be taken into account that the company receives over 11,000 customer service cases daily. Although the company's customer service receives continuous data protection training, the human factor can sometimes lead to a matter being answered as a customer service case instead of a response to a request under the GDPR referred to in Article 12(4), especially when the user does not mention personal data or the GDPR in his communication with the company.

The investigation has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Portugal, Belgium, Cyprus, Austria, France, Germany, Slovakia, Italy, Spain, Denmark, Norway and Finland.

Justification of the decision

The assessment of the Authority for Privacy Protection (IMY)

Has the company had the right to continue processing the complainant's data after the complainant objected to the processing?

According to Article 17(1)(c), 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 when the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing. According to Article 21(1) the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on Article 6(1)(f). The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

The complainant's email to the company of 24 May 2018 must be understood as an objection to the processing pursuant to Article 21(1), for reasons related to his specific situation, being that the card number cannot be reused to register new free trial periods on the company's services. Since the objection had not been handled before the introduction of the GDPR on 25 May 2018, the company's processing of requests must be assessed in accordance with the GDPR, i.e. whether the company has

demonstrated compelling legitimate grounds for processing that outweighs the interests, rights and freedoms of the data subject.

In order for processing to be based on Article 6(1)(f), all three conditions provided therein must be fulfilled, namely, firstly, that the controller or third party has a legitimate interest (*legitimate interest*), secondly that the processing is necessary for purposes of legitimate interest (*necessary*) and third that the interests or fundamental rights and freedoms of the data subject do not weigh heavier and require the protection of personal data (*balance of interest*).

Among other things, the company has stated that the company's *legitimate interest* with the processing is to counteract fraud regarding free trial periods. Recital 47 of the GDPR states that processing of personal data that is absolutely necessary to prevent fraud constitutes a *legitimate interest in* the controller concerned. IMY therefore considers that the company has a legitimate interest.

Furthermore, IMY believes that processing is absolutely *necessary* for purposes relating to legitimate interest. The investigation shows that the data has been minimised insofar as it is possible for the company to achieve the purpose of the legitimate interest.

In the *weighing of interests* to be made between the Company's legitimate interest and the interests, rights and freedoms of the complainant, IMY notes that *the company's legitimate interest* weighs heavily. The processing appears as something that the complainant can reasonably expect when registering a free trial and not particularly privacy invasive. The personal data in question can neither be considered as sensitive from a privacy perspective. In a summarized assessment, IMY finds that the company has demonstrated compelling legitimate grounds that outweigh *the complainant's interest in* the reuse of his card information to register new free trial periods on the company's services and that his personal data shall not be processed.

In light of the reasons the company has presented, IMY finds that the company has demonstrated compelling legitimate grounds that outweigh the complainant's interests, freedoms and rights. The Company has thus had the right to continue processing the data after the complaint has objected to the processing and the complaint has therefore not been entitled to erasure under Article 17(1)(c) GDPR.

Has the company handled the complainant's requests in a formally correct manner under the GDPR?

According to Article 12(1) of the GDPR, the controller shall take appropriate measures to provide any communication under Article 17 and 21 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Pursuant to Article 12(3) the controller shall provide information on action taken on a request under Article 17 and 21 to the data subject without undue delay and in any event within one month of receipt of the request. If the controller does not take action on the request of the data subject the controller shall pursuant to Article 12(4) inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. According to Recital 59 of the GDPR, the controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

In the present case, the legality of the Spotify's actions shall only be assessed during the period when the GDPR has been applicable, i.e. since 25 May 2018. However, when assessing whether the company has fulfilled its information obligations to the complainant through its reply on 8 June 2018, the answers that the company previously submitted to the complainant shall be taken into account for the company's benefit.

Spotify has stated, among other things, that the reason why the company in its reply to the complainant has not informed of its legal basis for the processing, its balancing of interests or the possibility to complain to supervisory authorities was due to the fact that the complainant did not mention personal data or the GDPR in his communications with the company and that the complainant shortly before received information about this through the company's privacy policy that came into force on 25 May 2018. However, IMY notes that the complainant expressly stated that his concern was about credit card information and for what purposes he meant that the data may be processed, which can hardly be understood as other than personal data and references to data protection rules. As stated above and as the company itself has found, the complainant's request must also be perceived as an objection pursuant to Article 21, which has thus entailed an obligation for the company to take an individualised decision to complainant pursuant to the GDPR. Since the company's decision was negative, the company should have informed of the reasons for its decision in accordance with Article 12(4) and included information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy, which it did not. What the company has stated that information about this has been disclosed by the company's privacy policy is not sufficient. This because the matter concerns an individualised decision and a data subject cannot be expected to review such a policy in its entirety to deduce what type of decision the company has made, especially when the company's response neither provided the legal basis for which the processing was based or information that an objection pursuant to the GDPR from the complainant had been rejected.

Against this background, IMY finds that the company's response of 8 June 2018 has not been sufficiently justified pursuant to Article 12(4) because the company has not clearly stated what personal data is being processed, that the data is processed on the basis of a legitimate interest and what the legitimate interest is and that the answer has not contained information about the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. Spotify has thus processed personal data in violation of Article 12(4) GDPR.

Choice of corrective measure

Articles 58(2) and 83(2) of the GDPR states that IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) lists which factors should be taken into account in deciding whether to impose an administrative fine and on the amount of the fine. If it is a minor infringement, IMY may, as stated in recital 148 instead of impose an administrative fine, issue a reprimand pursuant to Article 58(2)(b). Consideration shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous relevant infringements.

In its defence, the company has mainly stated that it is a one-time occurrence and that the company handles a large number of customer service matters. Furthermore, since the company's customer service advisors have undergone further training on how to answer users in a clear and clear manner, which questions should be considered as inquiries under the GDPR and what questions should be forwarded to the company's data protection team and data protection officer.

In an overall assessment of the circumstances, IMY finds that the stated infringements are minor violations in the sense referred to in recital 148 and that Spotify AB therefore should be issued a reprimand in accordance with Article 58(2) of the GDPR for the stated infringements.

This decision has been made by Head of Unit [REDACTED] after presentation by legal advisor [REDACTED]

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-03-24, no. DI-2020-10541. Only the Swedish version of the decision is deemed authentic.

Rebtel Networks AB
Org. no:556680-3622
Jakobsbergsgatan 16
111 44 Stockholm

Our ref.:
DI-2020-10561, IMI no. 120408

Date:
2021-03-23

Supervision under the General Data Protection Regulation – Rebtel Networks AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Rebtel Networks AB has processed personal data in violation of

- Article 17 of the General Data Protection Regulation (GDPR)¹ by not without undue delay having erased the personal data on 9 November 2020 that the complainant had requested erasure of 18 September 2019.
- Article 12(3) of the GDPR by providing incorrect information on 22 September 2019 that the complainant's data had been erased due to the complainant's request of 18 September 2019.

The Swedish Authority for Privacy Protection (IMY) issues Rebtel Networks AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Report on the supervisory matter

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Rebtel Networks AB (the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Spain) in accordance with the Regulation's provisions on cooperation in cross-border processing.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

The complaint states that the complainant has unsuccessfully tried to persuade the company to stop sending non-requiring emails after she removed her account. She has on four occasions requested removal and the company has each time confirmed that her data has been deleted and that she would not receive any more messages, but she then receives a new e-mail each time asking her to provide feedback about the service. She has also tried to use the "unregister" link listed in each email, but it has

¹Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

not worked either. Against this background, she believes that the company has violated its obligations under Article 17 of the GDPR.

Rebtel Networks AB has mainly stated the following.

The company received a request for deletion from the complainant on 18 September 2019. In retrospect, however, it can be noted that it has not been handled as a request for erasure under the GDPR, even if certain data were erased. This is why additional e-mails in the form of reminders of a customer survey survey have been sent to the complainant. This has been done during the period up to and including 1 October 2019, i.e. not after the one month deadline that applies under the GDPR to meet a request for erasure.

The remaining data was erased on 9 November 2020, except for those necessary to handle the current supervisory matter. The company informed the complaint on 20 November 2020.

Due to this supervisory matter, the Company has taken special measures to strengthen its established processes and procedures for identifying a request under the GDPR. This mainly includes further training of its customer service agents. The company has further improved its so-called data triggers in its customer service tool. The company's investigation of the complainant's case showed that it had not been flagged as a matter under the GDPR when the data application did not understand any reference to the GDPR in Spanish.

The processing has been done through correspondence. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Spain, Germany, Norway, Italy and France.

Justification of the decision

Applicable provisions

According to Article 12(3) of the GDPR, the controller shall, upon request, without undue delay and, in all circumstances, at the latest one month after receiving the request, provide the data subject with information on the measures taken pursuant to Article 17. If necessary, this period may be extended by an additional two months, taking into account the complexity of the request and the number of requests received. The controller shall notify the data subject of such an extension within one month of receipt of the request and indicate the reasons for the delay.

According to Article 17(1)(a), the data subject shall have the right to have their personal data erased by the controller without undue delay and the controller shall be obliged to erase personal data without undue delay if the personal data is no longer necessary for the purposes for which they were collected or otherwise processed. According to Article 17(3)(b), this shall not apply to the extent that the processing is necessary to fulfil a legal obligation requiring processing under Union law.

The assessment of the Swedish Authority for Privacy Protection (IMY)

Has there been an infringement of the GDPR?

The company has stated that the reason the complainant's request for erasure of 18 September 2019 was not handled until 9 November 2020 is because the company did not perceive it as a request for erasure.

In the opinion of the IMY, however, it has been clear from the request that the data subject wished to exercise her right to erasure. Since certain data was only erased on 9 November 2020, Rebtel Networks AB has processed personal data in violation of Article 17 of the GDPR by not without undue delay having erased the personal data on 9 November 2020 that the complainant had requested erasure of 18 September 2019. However, the company has had the right to retain the information needed to show that the request has been handled in accordance with the GDPR.

The Company has stated that no further e-mails have been sent since 2 October 2019 and that this is within the deadline of one month following Articles 12(3) and 17 GDPR. However, the company incorrectly stated in its reply to the complainant on 22 September 2019 that the information had been erased and that the complainant would not receive any more e-mails. Rebtel Networks AB has thus in violation of Article 12(3) the GDPR provided incorrect information about what measures – that the data had been fully erased – which had been taken due to the complainant's request.

Despite the fact that the company, on 22 September 2019, informed the complainant that no more e-mails regarding customer satisfaction would be sent, the complainant received another four such e-mails. The four e-mails were sent on 22 and 25 September, and on 1 and 2 October 2019. However, IMY notes that these were sent a relatively short time after the request for erasure was made and finds that it is within the timeframe that the company would have had to take action if the request had been handled correctly.

Choice of corrective measure

Articles 58(2) and 83(2) of the GDPR states that IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) lists which factors should be taken into account in deciding whether to impose an administrative fine and on the amount of the fine. If it is a minor infringement, IMY may, as stated in recital 148 instead of impose an administrative fine, issue a reprimand pursuant to Article 58(2)(b). Consideration shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous relevant infringements.

The company has stated that the reason the complainant's request for erasure was not handled correctly was mainly due to a mistake in the company's customer service and customer service tools. As a result of the incident, the company has stated that it has taken specific organisational and technical measures to strengthen its established processes and procedures, especially for identifying a request under the GDPR.

In an overall assessment of the circumstances, IMY finds that the stated infringements are minor violations in the sense referred to in recital 148 and that Rebtel Networks AB

therefore should be issued a reprimand in accordance with Article 58(2) of the GDPR for the stated infringements.

This decision has been made by Head of Unit [REDACTED] after presentation by legal advisor [REDACTED].

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-03-23, no. DI-2020-10561. Only the Swedish version of the decision is deemed authentic.

Boozt Fashion AB
Hyllie Boulevard 35
215 37 Malmö

Our ref.:
DI-2020-10544, IMI no. 115751

Date:
2021-06-17

Supervision under the GDPR – Boozt Fashion AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that the investigation in the matter does not show that Boozt Fashion AB has processed the complainant's personal data in violation of the GDPR¹.

The case is closed.

Report on the supervisory matter

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Boozt Fashion AB (the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Denmark) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The *complainant* states that the company has provided the complainant's e-mail address to third parties (Facebook) for the purpose of sending direct marketing to the complainant without having a legal basis for it. In December 2018, the complainant requested access pursuant to Article 15 of the GDPR from Facebook, which revealed that the company has disclosed the complainant's personal data to Facebook.

Boozt Fashion AB has mainly stated the following. The company is not the controller for the processing that the complaint concerns since the company's processing of the complainant's e-mail address took place before the application of the GDPR. The complainant's e-mail address was collected in 2016 in connection with a purchase from the complainant. In 2017, the complainant's email address was sent to Facebook in order to be able to target marketing using Facebook's custom audience function. This process was carried out in accordance with the current legislation. In spring 2018, before the introduction of the GDPR on 25 May 2018, Facebook changed its terms for the custom audience function. The company did not accept the terms and conditions and Facebook set the personal data that the company has transferred to Facebook in

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

¹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (GDPR).

quarantine while waiting for the company to accept the new terms. The company did not give Facebook any instructions to quarantine the personal data, but the initiative came from Facebook. During this period, the Company did not have access to or the possibility to use, modify or delete the personal data. The company approved Facebook's new terms in January 2019 and the quarantine personal data was then unlocked by Facebook, after which the company deleted the complainant's information. The company believes that the reason for the complainant's excerpt at Facebook in December 2018 revealed that the company had transferred the complainant's personal data to Facebook because that information remained from the transfer in 2017.

The company disputes that any processing of the complainant's personal data for direct marketing purposes has taken place, neither during the time when the personal data was quarantined by Facebook or during the time the GDPR has been applicable. According to the company, the company is only the controller for the transfer of the complainant's personal data to Facebook and for any direct marketing that has taken place before the personal data was quarantined, i.e. before the GDPR began to apply. Furthermore, the company has stated that during the period of the GDPR, the company has only processed the data subjects' personal data for direct marketing with their prior consent.

The investigation has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, France, Italy, Norway, Germany, Spain, Austria, Poland and Finland.

Justification of the decision

The assessment of the Authority for Privacy Protection (IMY)

Processing of personal data

According to Article 4(2) of the GDPR, 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Examples thereof is collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller

The controller, according to Article 4(7) of the GDPR, is the person who alone or together with others determines the purposes and means for the processing of personal data. If two or more controllers jointly determine the purposes and means of processing, they are joint controllers. According to Article 26, they are then obliged to establish their respective responsibilities in order to fulfil their obligations under the GDPR under an open form, through mutual arrangements. This means that the arrangement between the responsible parties must contain specific information about how the obligations under the regulation are to be fulfilled in practice. If there is no clarity as to how the obligations should be fulfilled, especially with regard to the rights of data subjects, both parties may be deemed to be acting in violation of Article 26(1) of the GDPR.

The purpose of these rules is to ensure that the responsibility for compliance with data protection rules is clearly distributed in cases where several actors participate, to avoid the reduction of the protection of personal data and lead to loopholes where certain obligations are not met by any of the parties involved in the processing.²

The Court of Justice of the European Union has stated in the case *Wirtschaftsakademie* that a common responsibility does not necessarily mean that the various actors involved in the processing of personal data have an equal responsibility.³ The actors can be involved in different stages of treatment and to different extents. The responsibility for each of them shall be assessed taking into account all relevant circumstances in the case.

In the *Fashion ID* case, the Court of Justice of the European Union concluded that a website operator using plugins on its website that enables website visitors' personal data to be transferred to a social media provider may be considered to be joint data controller with the social media provider.⁴ The court stated that the responsibility is limited to the parts of the processing chain for which the website operator actually determines the purposes and means for. In this case, the European Court of Justice considered that the website operator was only involved in determining the purposes and funds for collection and disclosure by transferring personal data about its visitors to the social media provider. The website operator was not considered responsible for the later measures carried out by the social media provider after the data had been disclosed to the latter, as the website operator was not involved in determining the purposes and means of subsequent processing.⁵

The company has stated that it has been the controller for the collection and transfer of the complainant's personal data to Facebook before quarantining the data. The question is therefore whether the company has been jointly controller during the time the personal data was quarantined, i.e. from spring 2018 (before the introduction of the GDPR and when Boozt did not approve Facebook's conditional changes) until January 2019 (when the personal data was erased).

The company transferred the complainant's email address to Facebook for the purpose of direct marketing to the complainant. From the moment the personal data was locked by Facebook, no direct marketing has been made to the complainant. Since the company did not approve Facebook's conditional amendments, it could not continue to process the personal data for the purpose it was transferred to Facebook. The company also did not instruct Facebook to store the personal data in quarantine. In the circumstances, the purpose of the processing seems to have changed when Facebook unilaterally decided to quarantine the complainant's personal data. This indicates that Facebook alone determined the purpose and means of processing and that Facebook has been solely responsible for the continued processing (storage).

When it comes to assessing the distribution of responsibilities between a controller who collected and transferred personal data to a social media provider for the purpose of direct marketing and the social media provider, several factors may be relevant. For example, the ability to influence the processing on a practical level, as well as the actual knowledge (or the knowledge they should have had) of each of the joint

² European Data Protection Board's (EDPB) Guidelines 07/2020 on the concepts of controller and processor in the General Data Protection Regulation, paragraph 160.

³ European Court of Justice ruling of 5 June 2018, *Wirtschaftsakademie*, case C-210/16, paragraph 43.

⁴ The European Court of Justice's judgment of 29 July 2019, *Fashion ID*, case C-40/17, paragraph 85.

⁵ *Fashion ID*, item 76.

controllers.⁶ However, it is not required that each operator in a joint processing has actual access to the personal data concerned in order to be considered jointly responsible.⁷

In the present case, it has not been shown that the company had the opportunity to dispose of the data or affect the processing of the data while quarantined.

Furthermore, the company has stated that it lacked knowledge of whether Facebook has directed direct marketing to the complainant while the personal data was locked.

In an overall assessment of the circumstances, IMY finds that the company cannot be regarded as a joint data controller while the personal data was locked by Facebook.

Conclusion

This supervision covers only the company's processing of the complainant's personal data in accordance with the GDPR.

The investigation has shown that the company's processing of the complainant's personal data has taken place before the application of the GDPR. From the time the complainant's personal data was quarantined by Facebook, which occurred before the application of the GDPR, the parties joint data controllership ceased resulting in that Boozt Fashion AB was no longer responsible for the continued processing of the complainant's personal data.

IMY therefore finds that the investigation in the case does not show that Boozt Fashion AB has processed the complainant's personal data in violation of the GDPR.

The case is closed.

This decision has been made by Head of Unit [REDACTED] after presentation by legal advisor [REDACTED]. The legal advisor [REDACTED] has also participated in the handling of the case.

Copy to

Counsel in the matter

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-06-16, no. DI-2020-10544. Only the Swedish version of the decision is deemed authentic.

⁶ EDPB's guideline 8/2020 on targeted advertising to social media users, point 133.

⁷The European Court of Justice's judgment of 10 July 2018, Jehovah Todistajat, case C25/17-, paragraph 69.

Smartphoto Nordic AB
Östergatan 39
211 22 Malmö

Our ref.:
DI-2020-11216, IMI no. 155145

Date:
2021-06-16

Supervision under the GDPR – Smartphoto Nordic AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Smartphoto Nordic AB has processed personal data in violation of

- Articles 12(3) and 17(1) of the General Data Protection Regulation (GDPR)¹ by not until August 2019 erasing the personal data that the complainant has requested erasure of 27 August 2018, and thereby not without undue delay, and
- Article 6(1) of the GDPR by having made a direct-addressed mailing to the complainant in August 2019 without a legal basis for the processing.

The Swedish Authority for Privacy Protection (IMY) issues Smartphoto Nordic AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Report on the supervisory matter

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Smartphoto Nordic AB (the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the GDPR, from the supervisory authority of the country where the complaint has lodged (Finland).The handover has been made in accordance with the provisions of the Regulation on cooperation in cross-border processing.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

The complaint is essentially the following. On 27 August 2018, the complainant requested that the company erase her personal data because she had stopped being a customer (the first request).The company didn't answer. On 18 May 2019, the complainant requested a new deletion (the second request).The company then responded that its IT department would handle the request. In August 2019, the complainant received a direct marketing letter from the company and therefore

¹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

assumes that the company has not deleted her personal data. The company has not provided any information about the measures taken.

Smartphoto Nordic AB has mainly stated the following.

The company handled the first request as a customer complaint. The company responded with a follow-up question if the complainant wanted compensation in the form of a new order of inducing images completely free of charge. This is part of the company's Satisfaction Guarantee where the company wants to make sure customers are satisfied with their order. The complainant did not respond to this request. In anticipation of response, the company waited to delete the account, as a new order is not possible after the account has been deleted.

When the complainant again made contact through the second request, deletion began two days later on 20 May 2019. The complaint received information about this the same day. The e-mail message stated, among other things, that this process can take up to 30 days before it is fully executed. After these 30 days, the complainant has not received any more mailings from the company except for an addressed direct mailing in the summer of 2019. These mailings are carried out a maximum of 2 times per year. The extract of addresses for the preparation of the mailing began during the 30 days where the process of erasing the complainant's information had begun but has not been fully executed. This meant that the complainant's account was still active regarding address and customer information when excerpts of addresses were made. Therefore, the complainant's address information was included as one of the recipients of the mailing. The company will review its procedures for excerpts of addresses when mailings so that it will not be repeated, so that accounts where deletion has begun shall not receive mailings.

The investigation has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Finland, Norway and Denmark. The *complaint* is essentially the following.

Justification of the decision

Applicable provisions, etc.

In order for the processing of personal data to be legal, a legal basis for processing is required in Article 6 of the GDPR.

According to Article 12(3), the individual's request to exercise his or her rights shall be handled without undue delay and in any event no later than one month after the request has been received. The deadline of one month may be extended by an additional two months if the request is particularly complicated or the number of requests received is high. If the period of one month is extended, the controller must notify the data subject of the extension. The notification of the extension of the deadline shall take place within one month of receipt of the request. The controller must also indicate the reasons for the delay.

According to Article 17(1)(a), the data subject shall have the right to have their personal data erased by the controller without undue delay and the controller shall be obliged to erase personal data without undue delay if it is no longer necessary for the

purposes for which they were collected or otherwise processed. Article 17(3) contains an exhaustive list of the exceptions to this right.

The assessment of the Authority for Privacy Protection (IMY)

IMY holds that it was clearly stated by the complainant's *first request* of 27 August 2018 that she wanted her personal data to be erased. The company was therefore obliged to delete the data unless there was a valid exception. Article 17(3) of the GDPR does not include any exceptions to offer, as the company has done, the data subject's compensation instead of deleting the data. Since there was no valid exception, the company was obliged to erase the data, which the company did not do until August 2019. The company has thus not erased the complainant's personal data without undue delay in the sense referred to in Articles 12(3) and 17(1). Against this background, there is no reason to decide on the measures taken by the company due to the second request of 18 May 2019.

Since the company was obliged to erase the data, the company has processed the complainant's personal data in violation of Article 6(1) of the GDPR by having made a direct-addressed mailing in August 2019 to the complainants without having a legal basis for the processing.

Choice of corrective measure

Articles 58(2) and 83(2) of the GDPR states that IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines shall be imposed in addition to or instead of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) lists which factors should be taken into account in deciding whether to impose an administrative fine and on the amount of the fine. If it is a minor infringement, IMY may, as stated in recital 148 instead of impose an administrative fine, issue a reprimand pursuant to Article 58(2)(b). Consideration shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous relevant infringements.

IMY notes that Smartphoto Nordic AB has deleted the data and that the company has reviewed its routines for direct-addressed mailings. The company has not previously received any corrective measure for infringement of data protection rules. In an overall assessment of the circumstances, IMY considers that there are minor violations in the sense referred to in Recital 148 and that Smartphoto Nordic AB should be issued a reprimand in accordance with Article 58(2)(b) of the GDPR for the stated infringements.

The case is closed.

This decision has been made by Head of Unit [REDACTED] after presentation by legal advisor [REDACTED].

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2021-06-16, no. DI-2020-11216. Only the Swedish version of the decision is deemed authentic.

Decision concerning a complaint

National Reference nr:
DI-2021-2067

IMI number:
184280

Date:
2021-08-31

[REDACTED] has lodged a complaint to the The Danish Data Protection Agency (Datatilsynet) against Nordic Entertainment Group Sweden AB's (NENT) for their handling of his request to access his data. Since NENT, who is the controller¹, has it's main establishment in Sweden, The Danish Data Protection Agency has handed over the complaint to the Swedish Authority for Privacy Protection (Integritetsskydds-myndigheten, IMY), in accordance with article 56.1 of the GDPR.²

IMY shall handle complaints and investigate, to the extent appropriate, the subject matter of the complaint (article 57.1 f of the GDPR).

[REDACTED] has requested that NENT should be ordered to provide the data by e-mail. NENT has refused to send the data by e-mail and stated that the data has been made available on [REDACTED] account. NENT has stated that they cannot ensure the proper protection of the personal data when sending it by e-mail.

Under article 5 of the GDPR, the controller shall be responsible for, and be able to demonstrate that the personal data is being processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In accordance with article 32 of the GDPR, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

IMY has no reason to doubt NENT's statement regarding that they cannot ensure the proper protection of the personal data when sending it by e-mail. For this reason IMY does not consider NENT to have acted in violation of the GDPR and thus finds no reason to order NENT to respond to the request by e-mail.

[REDACTED] has also stated in his complaint that NENT has failed to act on his request for access on time. NENT has admitted to being 8 days late to answer his request. [REDACTED] has now been offered access to his personal data, albeit not in the way he requested. NENT has stated that this breach has been remedied and that new routines have been put in place in order to prevent future delays. For this reason IMY sees no need to take any action on account of the delay.

The case is hereby closed.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

¹ Controller means the organisation (for example a corporation, foundation, association or authority) which determines the purposes and means of the processing of personal data. Thus, the controller is not the supervisor of a workplace or an employee. Natural persons can however sometimes be controllers, as in the case of sole traders. If two or more entities jointly determine the purposes and means of the processing, they have to decide between themselves who is responsible for the different obligations imposed by the GDPR. The controller can outsource the actual processing of personal data, but never transfer his or her responsibilities as controller.

² 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).

Decision Maker for IMY: [REDACTED] Legal Advisor

[REDACTED], 2021-08-31 (*Det här är en elektronisk signatur*)

Our ref.:
DI-2021-7331

Date:
2021-09-10

Final decision in IMI case register 134972

Decision of the Swedish Authority for Privacy Protection

The case will be closed without further action.

Background

A complaint was lodged with the UK SA on 20 September 2019. The complainant had bought a product in 2017 from a company that was later purchased by Irootfor (hereinafter the company). On three occasions in August 2019 (2nd, 4th and 20th), the complainant received marketing SMS from the company. In order to unsubscribe, the complainant had to text a non-UK number that would charge a fee according to the complainant. The complainant instead sent out a tweet (on Twitter) on 4 August which the company did not respond to. The complainant sent out another tweet on 20th August informing the company about potential fines for GDPR breaches. On 20th September 2019, the complainant received a fourth marketing text and sent out another tweet which the company responded to and offered removing the complainant's number from their database. The complainant requested that the company removed everyone's numbers and would otherwise file a complaint. The company informed the complainant that they have removed all numbers and would stop sending marketing SMS. On the question (from the UK SA complaint form) on what else the company could do in order to resolve the complaint, the complainant answered that the company should remove information of all customers who have not consented to receiving marketing SMS and issue a public apology.

Findings

Postal address:
Box 8114
104 20 Stockholm
Sweden
Website:
www.imy.se
E-mail:
imy@imy.se
Telephone:
+46 (8) 657 61 00

Firstly, we note that the complainant has used an informal way to contact the company (by a tweet on Twitter). It is understandable the complainant did not want to pay a fee in order to object to the marketing SMS but at the same time it is also understandable that the company did not give a formal response through Twitter directly. Most likely, there were other ways to contact the company (such as email) other than SMS. Secondly, we note that when the company responded to the complainant, they apologised for the text messages and removed the complainant's number. They also followed the complainant's request and removed all numbers in order to stop sending text messages. Accordingly, the issue seem to have been resolved and was probably due to a lack of communication in the contact through Twitter. In respect of the

complainant's requirement of a public apology, that is not something the GDPR regulates. We would also like to inform you that direct marketing by electronic communication is regulated by the Swedish Marketing Act (SFS 2008:486) over which the competent supervisory authority is the Swedish Consumer Agency. The demarcation between the Marketing Act and GDPR is yet not clear which means that there is the possibility that we are not even competent to handle the case.

Other remarks

Direct marketing by electronic communication is regulated by the Swedish Marketing Act (SFS 2008:486) over which the competent supervisory authority is the Swedish Consumer Agency. The demarcation between the Marketing Act and GDPR is yet not clear which means that there is the possibility the issue falls without the scope of our competency.

Conclusion

The Swedish SA considers the subject matter of the complaint investigated to the extent appropriate and that no further action is required. Accordingly, the case should be closed.

Notice. This document is an unofficial translation of the Swedish Authority for Privacy Protections (IMY) decision 2021-09-10, no. DI-2020-7331. Only the Swedish version of the decision is deemed authentic.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-01-19, no. DI-2021-4741. Only the Swedish version of the decision is deemed authentic.

Our ref.:
DI-2021-4741

Date of decision:
2021-12-19

Date of translation:
2022-01-20

Supervision under the General Data Protection Regulation – One.com Group AB

Final decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy protection finds that One.com Group AB has processed personal data in violation of Article 6(1)(f) of the GDPR¹ by processing data about the complainant's first name and surname, address, telephone number in confirmation e-mails, without it being necessary, for the legitimate interest of ensuring the identity of the person who changes contact details for a registered domain.

The Swedish Authority for Privacy Protection gives One.com Group AB a reprimand in accordance with Article 58(2)(b) of the GDPR.

Description of the supervisory case

The case handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision of One.com Group AB (One.com or the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as responsible supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged the complaint (Germany) in accordance with the Regulation's provisions on cooperation concerning cross-border processing.

The investigation at IMY has been carried out in written form. In the light of cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Poland, Norway, Ireland, Denmark, France and Italy.

The complaint

The complaint has, in essence, stated the following. The complainant wished to change the contact details (e-mail address) of a registered domain at One.com. The

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

¹ Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with respect to the processing of personal data and on the free flow of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

complainant contacted the company and informed that the previously registered e-mail address would need to be changed due to inactivity. The complainant was then asked to complete a form and attach a copy of their identity document. The e-mail address previously provided by the complainant had, at that time, been inactive for approximately three years. After the change of contact information (e-mail address) the company sent out a confirmation e-mail about the change to both the previous and the new e-mail address. The confirmation e-mail contained the complainant's personal data. Since the complainant has not been using the previously provided e-mail address for several years, they consider that the verification mailing to the previously given address is a violation of the GDPR. The complainant further states that they have not given consent to the processing and that the data may have been disclosed to unauthorized persons.

What One.com has stated

One.com has, in essence, stated the following.

One.com is the controller of the personal data concerned in the complaint.

It is correct that a confirmation e-mail is sent out when a domain owner wishes to change contact details (e-mail address). The e-mail contains the complainant's first name and surname, address, telephone number and e-mail address.

The company states that the lawful basis for sending personal data to both the previous and the new e-mail address is Article 6(1)(f) (legitimate interests). The purpose of the processing is to ensure the identity of the account holder, that changes to contact details (e-mail address) are done at the initiative of the account owner and to ensure that the holder of the new e-mail address receives information and accepts that it is linked to an account at One.com (this should be the same person). The company states that the procedure also ensures that the company fulfills its contractual obligations towards the account holder. Thus, according to the company, there is also a commercially justified purpose.

When an account is created on One.com, one of the main elements is the e-mail address to which the account is linked. The company informs anyone who creates a new account that the account is linked to the e-mail address provided by the account creator. The company, therefore, considers itself transparent with its personal data processing.

As the mailings only contain necessary, general personal data, the company states that the rights and freedoms of the data subjects do not override the legitimate purposes of the company.

As an account is linked to the e-mail address initially provided by the account creator, the company uses a copy of the account holder's identity document together with e-mail verification as a two-factor authentication. It is done to ensure that the change of contact details (e-mail address) is approved by the account holder and to ensure that the company complies with its obligations towards the account holder under the agreement. Only a copy of an identity document could not fulfil the same purpose.

Summary of the company's statements

The purpose of the data processing

The company states that they have an interest in processing personal data in the e-mail verification for the following purposes:

- to ensure the identity of the account holder;
- to ensure that the change of contact details takes place at the initiative of the account owner;
- to ensure that the account holder of the new e-mail address accepts that the address is linked to an account at One.com; and
- to ensure that the company complies with its contractual obligations towards the account holder.

The necessity of the data processing

The company states that the processing of personal data in the e-mail verification is necessary because:

- the e-mail verification is part of a two-factor authentication of the account holder;
- only a copy of the identification document does not fulfil the purpose of verification; and
- the company needs to verify that the change to the contact information has been initiated by the account holder.

Balancing of the legitimate purpose of the company and the rights and freedoms of the data subjects

The nature of the personal data

The email contains the complainant's first name and surname, address, telephone number and e-mail address, which does not constitute sensitive personal data.

Reasonable expectations

The company considers that the personal data processing in question is transparent in relation to account holders because the company informs those who open an account with One.com that the account is linked to the email address chosen.

The company's view is that the fundamental rights and freedoms of the data subjects do not therefore override the interests of the company.

Justification of decisions

Applicable provisions

In order for a personal data processing to be considered lawful, it is necessary that at least one of the conditions set out in Article 6(1) GDPR is fulfilled.

For processing to be able to rely on Article 6(1)(f), three conditions need to be filled: (1) the controller or third party has a legitimate interest (legitimate interest), (2) the processing is necessary for the purposes of the legitimate interest (necessary) and (3) that the interests or fundamental rights and freedoms of the data subject do not override and require the protection of personal data (balance of interests).

It follows from the case-law of the Court of Justice of the European Union that exceptions and limitations to the protection of personal data must be limited to what is strictly necessary.² Furthermore, the condition required by Article 6(1)(f) must be examined in conjunction with the principle of data minimisation (Article 5(1)(c)). This presupposes that the legitimate interest which the processing is intended to protect cannot reasonably be protected as effectively by other means which less adversely affect the fundamental rights and freedoms of data subjects, and that no more data than is necessary is processed.³

Recital 47 states that the legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing

Assessment of the Swedish Authority for Privacy Protection

IMY considers that the interests presented by the company are justified, having regard in particular the fact that the processing of personal data contained in the e-mail verification:

- is part of a two-factor verification;
- ensures that the change of contact details has been initiated by the account holder; and
- ensures that the holder of the new registered e-mail address accepts that the address is linked to an account at One.com.

IMY has now to consider whether all the personal data contained in the confirmation e-mails were necessary in relation to the purpose. IMY does not dispute that the company sent confirmation e-mails to the complainant's previously registered and new e-mail address based on the legitimate interest. However, IMY considers that the purpose of the confirmation e-mails, to ensure that the contact details are changed by the right person, can be achieved without mentioning the complainant's first name, surname, address and telephone number. Given that all the personal data contained in the confirmation e-mail were not necessary to protect the legitimate interest, the processing is not lawful on the basis of legitimate interests.

IMY therefore finds that One.com has violated Article 6(1)(f) of the GDPR by processing personal data in a confirmation e-mail without it being necessary in relation to the purpose of the processing.

² Case C-13/16 'Rīgas satiksme', Judgement of 4 May 2017, para. 30.

³ Case C-708/18 TK v Asociatia de Proprietari bloc M5A-ScaraA, Judgement of 11 December 2019, paras. 46-51. The Court of Justice has also confirmed that that case-law continues to apply in the context of the GDPR; Case C-597/19 M.I.C.M, Judgement of 17 June 2021, para. 107.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) IMY has the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the individual case, administrative fines may be imposed in addition to or instead of the other measures referred to in Article 58(2). Furthermore, Article 83(2) states which factors should be taken into account in decisions on whether administrative fines should be imposed and when determining the amount of the fine. In case of a minor infringement, IMY may, as stated in Recital 148, instead of imposing a sanction fee, issue a reprimand pursuant to Article 58(2)(b). In this assessment, regard shall be taken to aggravating and mitigating circumstances in the case, such as the nature of the infringement, severity and duration as well as previous infringement of relevance.

IMY notes the following relevant facts. The violation has affected one person and it has not concerned sensitive data. IMY has not previously established that the company has infringed the GDPR. Furthermore, the investigation has not shown that there has been any disclosure of personal data to a third party. One.com clearly informs its customers that they have an obligation to keep their contact details up to date.⁴ At the time of the change, the applicant's previous e-mail address had been inactive for about three years. In an overall assessment of the circumstances and the nature of the infringement, IMY considers that it is a matter of a minor infringement within the meaning of recital 148 and that One.com should be given a reprimand pursuant to Article 58(2)(b) of the GDPR for the stated infringement.

The case is closed.

This decision has been made by the specially appointed decision-maker [REDACTED]
[REDACTED] after presentation by legal advisor [REDACTED]

⁴ <https://www.one.com/en/terms-and-conditions-usd>

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Our ref.:
134935

Date:
2022-01-25

Complaint concerning H&M

Regarding the complaint against H&M in IMI case register no 134935, national reference no 5.15-0544-025/017-19/191 in the case lodged with the German SA (Niedersachsen).

Background

The complaint states that H&M had placed another customers list of order in the complainant's received package. Thus the complainant could see another customer's first and last name, full address (street, house number, postcode, city, country) order number and date, email address and payment method (Paypal). The complainant argues that by knowing that the payment method is Paypal - including knowledge of the email address - which is a part of the login process, the complainant could possibly get access to the email account with the help of the other data and thus reset the password securely at Paypal which also gives the complainant access to Paypal directly from this point of view. The complainant finally argues that the list of order also contains a detailed list of another customer's order, including underwear which the complainant consider to be highly questionable. Not the clothes themselves, but the situation could be really unpleasant for the concerned customer unknown to the complainant.

Finding

The Swedish Data Protection Authority (DPA) finds that the alleged data protection violations does not involve actual processing of the complainant's personal data. Since it does not involve the processing of the complainant's data, it is not an actual complaint pursuant to article 77 of the GDPR that require the Swedish DPA to investigate the subject matter to the extent appropriate pursuant to article 57(1)(f). However, the information provided will be used in the Swedish DPAs general planning of future supervision.

With this informational letter the case will hereby be closed.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 657 61 00

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision 2021-12-17, no. DI-2020-10525. Only the Swedish version of the decision is deemed authentic.

Ref no:
2020-10525
IMI case no. 101348

Date of decision:
2022-02-16

Date of translation:
2022-02-17

Supervision under the General Data Protection Regulation – Nordnet Bank AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Nordnet Bank AB has processed personal data in breach of Article 12(2) of the General Data Protection Regulation (GDPR)¹ by requiring the complainants, in complaint 1 and 2, to submit data in order to prove their identities via regular mail, even though Nordnet Bank AB had a digital service (communication centre) for other customer communications that require identification. Nordnet Bank AB has thus not sufficiently facilitated the exercise of the data subjects' rights.

The Swedish Authority for Privacy Protection issues Nordnet Bank AB a reprimand in accordance with Article 58(2)(b) for the infringement of Article 12(2) of the GDPR.

Report on the supervisory matter

The procedure

The Authority for Privacy Protection (IMY) has initiated supervision regarding Nordnet Bank AB (Nordnet or the company) due to two complaints. The complaints have been submitted to IMY, as responsible supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Finland) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of complaints relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Norway, and Finland.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

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).

What is stated in the Complaints

Complaint 1 (Finland with national registration number 2188/182/18)

The complainant contacted the company on 25 May 2018 regarding a request for access. The company required the complainant to send the request by e-mail with a copy of their ID document, which means that the copy may need to be signed and scanned. The complainant is of the view that Nordnet hinders the exercise of the right of access and refuses to act upon a request.

Complaint 2 (Finland with national registration number 3251/182/18)

The complainant has filed a complaint to the Finnish Data Protection Authority on 14 June 2018 after contacting the company regarding a request for access. Nordnet required the complainant to submit a signed request in writing together with a copy of a valid identification document. The company denied the complainant to use the web service for exercising the right of access. It is further stated that the company's web service already has high requirements for identification as it is a business in the financial sector. The complainant wonders whether the company can refrain from acting on a request for access that is attached and sent via its web service and argues that the company makes the exercise of the right of access more difficult.

What Nordnet Bank AB has stated

Nordnet Bank AB has essentially stated the following. Nordnet Bank AB is the data controller for the processing operations to which the complaint relates.

To be able to exercise the right of access the complainants were required to use regular mail (i.e. as opposed to digital ways of communications) to submit the following data; date, place, name, signature and a certified ID copy. The company needed the information to be able to identify the data subject to whom the request relates (name and ID copy respectively), to be able to determine when the request has been made (date), and to ensure that it is the data subject himself who is exercising the right of access (signature and ID copy respectively).

As a bank, Nordnet needs to apply strict rules on identification, *inter alia* because of the statutory banking secrecy which means that the company may not disclose or hand out information about a customer or a customer relationship to anyone other than the customer itself.

At the time of the complaints, Nordnet referred to special forms available on the company's website. The data subjects were asked to fill in the form and attach a certified ID copy and send the documents to the company by post. The company is of the view that the complainant's statement that the request of access should be made by e-mail is incorrect.

When the company carried out a control activity, the Data Protection Officer noted that the existing procedures regarding the right to access by data subjects and to receive a copy of their data should be harmonised with how other communications with customers are handled, and thus be able to be received through the company's online customer service in line with the majority of other customer communications that require identification. New procedures for digital management of the data subject right to access the personal data were implemented accordingly in February 2020 and

requests are now received through the company's online customer service in line with other customer communications that require identification. The change makes it easier for customers to exercise their rights under the GDPR.

Justification of the decision

Applicable provisions, etc.

According to Article 5(1)(c) GDPR, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

According to Article 11(2) where in the cases referred to in paragraph 1 of this article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling the identification.

Article 12(2) requires the controller to facilitate the exercise of the data subject's rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

Article 12(6) provides that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The assessment of the Swedish Authority for Privacy Protection (IMY)

On the basis of the complaints in this case, IMY examined the company's conduct in these individual cases. Therefore, IMY will not consider whether the company's current procedure for processing requests is compatible with the GDPR, but may take into account possible improvements when considering choice of corrective measures.

General starting points

It can be concluded that, in order to identify a data subject, the controller may request additional information that is necessary, where the controller has reasonable grounds to doubt the identity of the person making the request.

The GDPR does not explicitly regulate what data may be requested or how the additional information is to be collected. The controller must carry out a proportionality assessment in order to determine what is appropriate with regard to the Regulation's requirements, inter alia, for security reason, but also in the light of the requirement in Article 12(2) GDPR, according to which the controller shall facilitate the exercise of the data subject's rights. IMY finds that, requiring data on a general basis for identification purposes irrespective of whether the data is necessary as described in Article 12(6) is

contrary to both this provision and also to the principle of data minimisation in Article 5(1)(c).

A copy of the ID document should not be requested unless it's necessary. It is only in cases where the actual identity is crucial that it could be relevant. Identification with an ID document is not necessary if the controller has not verified the correct identity of the data subject when the customer relationship was established. This means that if the controller has found it satisfactory that a customer has provided, for example, an e-mail address that does not contain the correct name when the customer's relationship was established, the controller should not require more personal data when the customer wants to exercise his or her rights.

In the light of the requirements of Article 12(2), it is only in exceptional cases acceptable for a controller to refer individuals to regular mail service as the sole route of contact when they are required to submit data in order to ensure their identities, for example if it is justifiable for security reasons. The outset should be that alternative means of submitting requested information should be offered. For example, if the controller already has digital contact service for customers that involves verification — as many controllers have for example, customer portals, messaging centres or so-called "My pages" etc. for other customer communications — it may be questioned why data subjects should be faced with a more cumbersome handling when exercising their rights under the GDPR without specific justification.

Has there been an infringement of the GDPR?

The question is whether the information required by the company — a signed request containing the date/place, name, and a certified copy of the identity document — was necessary to identify the respective complainant and whether the procedure for submitting the information offered by the company was in accordance with the GDPR.

Nordnet has been given the opportunity to justify the necessity of all the required personal data at issue and the reasons why the processing of the requests, including referring data subjects exclusively to regular mail, was justified in the present case. In summary, the company states that, as a bank, it needs to apply strict identification rules in order not to risk breaching banking secrecy laws. As regards to the handling of the data subjects' requests, the company states that, as the practice has evolved and interpretations were communicated by various European Supervisory Authorities, it has developed digital management when it comes to data subjects access to personal data, without further justifying the handling at the time of the cases in question.

In order to assess whether the information requested by the company for identification in respect of complaints 1 and 2 was necessary, account must be taken of the fact that the importance of secure identification is particularly important when individuals, as in the case, turn to a bank with a request for access. In addition, it must also be taken account, that under legislation on prevention of money laundering and terrorist financing, Nordnet is obliged to identify their customers and verify their identities when establishing customer relationship. Against this background, and the relatively small amount of personal data including the ID copy, the requested data cannot be considered unjustified. Nordnet Bank AB has therefore not violated Article 5(1)(c) or Article 12(6) of the GDPR.

However, IMY finds that, there has been no evidence which makes it justifiable to require the complainants to send the requested information to the company by regular

mail. In an overall assessment of all the circumstances, including that at the time of the complaints the company had a digital service through a messaging centre for other customer communications with identification requirements, IMY considers that Nordnet Bank AB acted in breach of Article 12(2) of the GDPR by requiring the data subjects to use regular mail to submit the required data to the company when exercising the right of access.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The company have taken measures for digital management of the data subject right to access and the infringement found occurred relatively long ago and affected two individuals. Furthermore, the company has not previously received any corrective measures for infringements of the data protection rules. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Nordnet Bank AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been made by the specially appointed decision-maker [REDACTED]
[REDACTED] after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-03-18, no. DI-2021-10488. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-10488

Date of decision:
2022-03-18

Date of translation:
2022-03-18

Decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that Klarna Bank AB has processed personal data in breach of Article 12(3) of the General Data Protection Regulation (GDPR)¹ by not without undue delay complying with the complainant's request for erasure pursuant to Article 17 of 25 November 2020 only on 24 January 2020.

The Authority for Privacy Protection issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(3) of the GDPR.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority pursuant to Article 56 of the General Data Protection Regulation (GDPR) from the supervisory authority in the Netherlands where the complainant has lodged their complaint in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Denmark, Austria, Italy, Poland, and Finland.

The complaint

The complainant has mainly stated she requested erasure under Article 17 of the GDPR, but that it took two months before she received a reply from Klarna. After two months, she has received a reply which states that her request will be handled and that her request for erasure may take another 90 days to be completed. The

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

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).

complainant considers it unreasonable that it takes a total of five months for Klarna to handle her request.

What Klarna has stated

Klarna has mainly stated the following.

Klarna is the data controller for the processing to which the complaint relates.

The complainant's request for erasure was received by Klarna on 18 November 2020, after which Klarna verified the applicant's identity on 25 November 2020 and on 26 November 2020 requested a confirmation of the initiation of the erasure process. On 27 November 2020 the complainant submitted a confirmation, but this has not been brought to the attention of the case handler. Klarna sent a further request for confirmation on December 2020. On 24 January 2021, Klarna informed the complainant that the erasure process had been initiated and that the processing was delayed due to lower staffing during the Christmas and New Year holidays. On the same date, the process of erasure of the complainant's personal data was completed.

Klarna holds that it has handled the complainants request without undue delay considering the Christmas and New Year holidays and the individual error concerning the confirmation. Pursuant to Article 12(3) of the GDPR, Klarna informed the complainant of the maximum period allowed for carrying out a deletion. The reason for this was that the number of incoming cases was sometimes very high and the processing during these times could take more than a month. Klarna further states that it has further developed the processes concerning data subjects' rights in order to ensure that the deadlines set are met and that the data subject is clearly informed. In addition, the responsible case officer in the case in question, as well as the other case officers, have received additional information on the importance of careful and expeditious handling of these cases.

Justification of the decision

Applicable provisions, etc.

Article 12(3) of the GDPR requires the controller to provide the data subject, upon request, without undue delay and in any event no later than one month after receiving the request, with information on the actions taken pursuant to, inter alia, Article 17. The one-month time limit may be extended by a further two months where the request is particularly complex or the number of requests received is high. If the time limit of one month is extended, the controller shall inform the data subject of the extension. Notification of the extension of the deadline shall take place within one month of receipt of the request. The controller shall also indicate the reasons for the delay.

European Data Protection Board (EDPB) Guidelines 01/2022 on access state that the time limit starts when the controller has received a request. However, when the controller needs to communicate with the data subject due to the uncertainty as to the identity of the person making the request, there may be a suspension in time until the controller has obtained the information needed from the data subject, provided the controller has asked for additional information without undue delay.²

² EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, adopted for public consultation on 18 January 2022

Article 17(1)(a) provides that the data subject shall have the right to have his or her personal data erased without undue delay from the controller and the controller shall be obliged to erase personal data without undue delay if they are no longer necessary for the purposes for which they were collected or otherwise processed. Article 17(3) lists exhaustively the exceptions to this right.

Assessment of the Authority for Privacy Protection (IMY)

The investigation shows that the complainant's request for erasure was received by Klarna on 18 November 2020. Since Klarna had to communicate with the complainant in order to secure their identity and requested additional information without undue delay, IMY considers that the time limit to start again once the identity of the complainant has been verified on 25 November 2020. According to Klarna, the request has been fully met on 24 January 2021, which IMY does not find any reason to call into question.

Klarna did not inform the complainant until 24 January 2021, i.e. approximately two months after the request was received and the identity of the complainant was verified, that the erasure process was initiated and that it can take up to 90 days for the erasure to be completed as well as stated the reasons for the delay. IMY therefore concludes that Klarna has not dealt with the complainant's request without undue delay within the meaning of Article 12(3) of the GDPR.

In light of the above, IMY concludes that Klarna has processed the complainant's personal data in violation of Article 12(3) of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine.

In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The handling of the complainant's request has been delayed mainly due to an individual procedural error. The violation is due to human error and has affected only one person. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Klarna Bank AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-05-11, no. DI-2021-10263. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-10263, IMI case no.
185203,
LDA-1085.1-1399/20-F

Date of decision:
2022-05-11

Decision under the General Data Protection Regulation — Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that Klarna Bank AB is processing personal data in breach of Article 15 of the General Data Protection Regulation (GDPR)¹ by not complying with the complainant's request of 22 December 2019 for information about the recipients to whom his personal data have been disclosed.

The Authority for Privacy Protection issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 15 of the GDPR.

Report on the supervisory case

The case handling

The Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna) due to a complaint. The complaint has been submitted to IMY, in its capacity as lead supervisory authority under Article 56 of the General Data Protection Regulation (GDPR). The handover has been made by the supervisory authority of the country where the complainant has lodged his complaint (Germany) in accordance with the Regulation's provisions on cooperation concerning cross-border processing.

The investigation in the case has been carried out through correspondence. Since the complaint regards cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Denmark, Austria, Italy, Poland, and Finland.

The complaint

The complainant mainly states the following.

He has requested access to his personal data under Article 15 of the GDPR. The information he obtained from Klarna did not include all the information that he had

Postal address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Telephone:
08-657 61 00

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).

asked for since it lacked information about the recipients to whom his personal data had been disclosed. Even though the complainant came back with a request to know exactly which recipients his data had sent to, Klarna has not complied with this request.

Due to the complaint, IMY has initiated supervision in order to examine if the complainant's request has been complied with in accordance with Article 15 of the GDPR.

What Klarna has stated

Klarna states that it is the controller for the processing to which the complaint relates.

The information sent to the complainant on the 24th of January 2020 is in accordance with the obligations of the GDPR. Klarna has no duty to reply to the complainant's access request in any other way than it did. The EDPB Guidelines 01/2022 on access was adopted on the 18th of January 2022, i.e. two years after the complainant's case regarding access request was closed.

Justification of the decision

Applicable provisions, etc.

Article 15 of the GDPR provides that the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data. The data subject shall also have the right to information about the recipients or categories of recipient to whom the personal data have been or will be disclosed (Article 15(1)(c)).

Article 19 of the GDPR requires the controller to communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

According to Article 5 the controller shall be responsible for, and be able to demonstrate compliance with, inter alia the obligation to process personal data fairly and in a transparent manner in relation to the data subject.

EDPB Guidelines 01/2022 on access state that concerning the question, if the controller is free to choose between information on recipients or on categories of recipients, it has to be recalled, that, already under Art. 13 and 14 GDPR information on the recipients or categories of recipients should be as concrete as possible in respect of the principles of transparency and fairness. The controller should therefore generally name the actual recipients unless it would only be possible to indicate the category of recipients. Nevertheless, sometimes naming the actual recipients is not yet possible at the time of the information under Art. 13 and 14 GDPR but only in a later stage, for example when an access request is made. The EDPB recalls in this regard,

that storing information relating to the actual recipients is necessary *inter alia* to be able to comply with the controller's obligations under Art. 5(2) and 19 GDPR.²

Assessment of the Authority for Privacy Protection

The wording of Article 15(1)(c) of the GDPR does clarify if the controller is free to choose between information on actual recipients or on only categories of recipients.

However, IMY concludes that Article 15(1)(c), read together with Article 19 and in light of the principles of fairness and transparency (Article 5(1)(a)) cannot be interpreted any other way than as a right of the data subject to, especially when explicitly requested, obtain from the controller information about the actual recipients to whom the personal data have been or will be disclosed, unless this proves impossible or involves disproportionate effort.

IMY notes that the complainant has explicitly requested information about actual recipients. Klarna has not proved that this has proven impossible or to involve disproportionate effort. Klarna has thus processed the complainant's personal data in violation of Article 15 of the GDPR.

What Klarna has stated about that the EDPB Guidelines on access was adopted after the access request was complied with, does not lead to any other conclusion. IMY does not claim that Klarna has an obligation to comply with guidelines that was not available to Klarna at the time of the violation. IMY's reason for citing the guidelines is to prove that there is wide support for IMY's opinion, which follows from the wording of Article 19.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine.

In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes that the violation has affected one person and has not involved sensitive data. Furthermore, Klarna has otherwise complied with the complainant's request for access. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Klarna Bank AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR for the established infringement.

² EDPB Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, adopted for public consultation on 18 January 2022, paragraph 115.

This decision has been approved by the specially appointed decision-maker [REDACTED]
[REDACTED] after presentation by legal advisor [REDACTED]

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-05-13, no. DI-2021-6140. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-6140 ,IMI. Case no.
186981, A60FD 399045

Decision under the General Data Protection Regulation– Volvo Personvagnar AB

Date of decision:
2022-05-13

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Volvo Personvagnar AB has processed data in breach of

- Articles 12(3) of the General Data Protection Regulation (GDPR)¹ by not without undue delay responding to the complainant's request for access pursuant to Article 15 of GDPR, the 25 February 2020 only on 15 September 2021.

The Swedish Authority for Privacy Protection issues PUA a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(3) of the GDPR.

Report on the supervisory report

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Volvo Personvagnar AB (the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR) from the supervisory authority in the Ireland where the complainant has lodged their complaint in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Finland, France, Ireland, Italy, the Netherlands, Norway, Poland, Portugal and Hungary.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

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).

The complaint

In March 2019, the complainant requested access to his personal data pursuant to Article 15 of the GDPR. The applicant requested, inter alia, information on warranty repairs, carried out by a car brand repair shop belonging to the company (the car repair shop). The company replied that information on warranty was not available from the company.

What Volvo Personvagnar AB has stated

The company has mainly stated the following.

The company is the data controller for the processing to which the complaint relates.

On 25 February 2020, the complainant submitted a request for access to personal data. The request concerned, inter alia, an invitation to provide information on the servicing of the complainant's vehicle.

On 3 March 2020, the car repair shop sent the complainant a copy of a service invoice.

On 24 March 2020, the company sent a copy of the personal data containing information on the warranty repairs carried out, service on the vehicle and technical reports on the vehicle.

On 2 April 2020, the complainant lodged a complaint to the company alleging that the car repair shop had indicated that the information on the warranty repair, could not be disclosed.

On 14 April 2020, the complainant clearly stated that he wishes to have access to, inter alia, the following information:

- correspondence between the complainant and the company's customer service/carrier;
- correspondence between the complainant and the workshops concerning the vehicle in question;
- marketing; and
- recall of vehicles;

On 17 April 2020, the complainant received correspondence as set out above. At the same time, the company asked the complainant to clarify its request concerning marketing information and requests for correspondence with which country's customer service was the subject of the request.

On 14 May 2020, the complainant received a copy of the correspondence between the complainant, car repair shops and the company.

On 17 June 2020, the complainant requested information on warranty repairs from the company.

On 28 August 2020, a copy of the personal data was sent to the complainant with the following information on:

- correspondence from the company's customer service in the United Kingdom;
- correspondence from the local Irish sales office including, inter alia, the date of the warranty repairs carried out;

- service performed for which the company has information, the vehicle (date of technical reports on the vehicles); and
- a statement from a lawyer working for the company concerning what information the company doesn't have and that the applicant needs to contact the car repair shop concerned.

On 4 September 2020, the company informed the complainant that the company had requested the relevant car repair shop to provide information on service and warranty repairs.

On 15 September 2021, the DPO sent a letter to the complainant and apologised for the handling of the request for information on warranty repair. In its reply, the company attached the following information.

Data from the system QV90:

- service history (date, metering, workshop and dealer),
- roadside assistance insurance from the local system;
- the next service date according to service intervals;
- listing in free text about measures and warranty cases (date, metering, warranty case, so-called QB number), missing component, applied for costs from the workshop for work and materials, cost allocation (between sales company/importer and manufacturer).

Information from the system of technical records from the time when the complainant owned the vehicle, as follows:

- logs on the vehicle where it has been recorded in technical reports;
- possible warranty cases (errors/problems that may occur on this vehicle and on which it is possible to call for a guarantee);
- logs on completed warranty cases, reports such as problems with the vehicle where the workshop involves the support of the sales company and/or the support company. These reports are linked to the vehicle and the complainant.

The company submits that the car repair shops are independent of the company. It is the car repair shops that have carried out warranty and service work on the complainant's vehicles. It is for the car repair shops to provide the complainant with information on warranty and service work, as the workshops own the customer relationship and hold relevant information and data on such works. The complainant therefore needed to have a direct dialogue with the car repair shop on information concerning warranty and service provided. The company does not handle service or service invoices. Service is provided by the independent car repair shop and the car repair shop is data controller for the service information.

The company points out that the reason why the data from the QV90 system and the technical notes were not sent to when the complainant in the first communication was due to the human factor. The company has now ensured that the mistake will not happen again.

The company has been in constant communication with when the complainant and has attempted to respond to its various requests. The company points out when the complainant sought, in essence, information relating to the car repair invoice for a particular warranty and service work carried out, which is information to which the company did not have access to.

Justification of the decision

Applicable provisions, etc.

Concept of personal data

According to Article 4(1) of the GDPR, '*personal data*' means any information relating to an identified or identifiable natural person ('*data subject*'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

The concept of 'personal data' may include all information, whether objective or subjective, provided that it 'relates' to a particular person, which it does if, by virtue of its content, purpose or effect, it is linked to that person.²

In the judgment of the Court of Justice of the European Union in *Valsts ienēmumu dienests*, the Court held that the information requested by the Latvian tax authority, in particular data relating to the chassis numbers of the vehicles advertised on the operator's web portal, constitutes personal data within the meaning of Article 4(1) of the GDPR.³

The European Data Protection Board (EDPB) Guidelines 01/2022 on data subject rights - Right of access, inter alia:

51. Additionally, the controller needs to assess whether the requests made by the requesting persons refer to all or parts of the information processed about them. Any limitation of the scope of a request to a specific provision of Art. 15 GDPR, made by the data subjects, must be clear and unambiguous. For example, if the data subjects require verbatim "information about the data processed in relation to them", the controller should assume that the data subjects intend to exercise their full right under Art. 15(1) – (2) GDPR. Such a request should not be interpreted as meaning that the data subjects wish to receive only the categories of personal data that are being processed and to waive their right to receive the information listed in Art. 15(1)(a) to (h). This would be different, for example, where the data subjects wish, with regard to data which they specify, to have access to the source or origin of the personal data or to the specified period of storage. In such a case the controller may limit its reply to the specific information requested.

104. The words "personal data concerning him or her" should not be interpreted in an "overly restrictive" way by controllers, as the Art. 29 Working Party already stated with regard to the right to data portability. Transposed to the right of access, the EDPB considers for example that recordings of telephone conversations (and their transcription) between the data subject that requests access and the controller, may fall under the right of access provided that the latter are personal data. [...]

150. It is the responsibility of the controller to decide upon the appropriate form in which the personal data will be provided. The controller can, although is not necessarily obliged to, provide the documents which contain personal data about

² Judgment of the Court of Justice of the European Union, Nowak, C-434/16, EU:C:2017:994, paragraphs 34-35.

³ Judgment of the Court of Justice of the European Union, Valsts, C-175/20, EU:C:2022:124, paragraphs 34 and 36.

the data subjects making the request, as such and in their original form. The controller can for example, on a case-by-case basis, provide access to a copy of medium given the need for transparency (for example, to verify the accuracy of the data held by the controller in the event of a request for access to the medical file or an audio recording whose transcript is disputed). However, the CJEU, in its interpretation of the right of access under the Directive 95/46/EC, stated that "for [the right of access] to be complied with, it is sufficient for the applicant to be provided with a full summary of those data in an intelligible form, that is, a form which allows him to become aware of those data and to check that they are accurate and processed in compliance with that directive, so that he may, where relevant, exercise the rights conferred on him". Unlike the directive, the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents. Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing. Hence, there is no contradiction between the wording of the GDPR and the ruling by the CJEU regarding this matter. The word summary in the ruling should not be misinterpreted as meaning that the compilation would not encompass all data covered by the right of access, but is merely a way to present all that data without giving systematically access to the actual documents. Since the compilation needs to contain a copy of the personal data, it should be stressed that it cannot be made in a way that somehow alters or changes the content of the information.

EDPB Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications, *inter alia*:⁴

3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts, location data or data collected by cameras may concern driver behaviour as well as information about other people who could be inside or data subjects that pass by. Such technical data are produced by a natural person, and permit his/her direct or indirect identification, by the data controller or by another person. The vehicle can be considered as a terminal that can be used by different users. Therefore, as for a personal computer, this potential plurality of users does not affect the personal nature of the data

29. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver's complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle

⁴ EDPB, Guidelines 01/2020 on processing staff data in the context of connected vehicles and mobility related applications, Version 2.0, adopted on 9 March 2021 following public consultation, paragraphs 3, 29 and 62; IMY translation

parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

62. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). [...]

In the preparatory work documents for the law '*Road infrastructure charges and electronic toll systems*', the legislature⁵ noted that the very broad definition of personal data was the subject of discussion in the legislative file which resulted in the Law on road traffic registers⁶ and stated the following. In the field of road traffic there are both personal data and vehicle technical data. However, in some cases it may be difficult to determine to which category a particular task falls. A technical data of a vehicle should not be considered as personal data if it cannot be linked to the identity of the owner of the vehicle. On the other hand, an indication that a particular vehicle is subject to a driving ban refers to the owner of the vehicle in a specific way and it is therefore likely to be personal data. In the light of this statement, the Government considered in the preparatory work for the Act on⁷ Congestion Tax that the registration number of a vehicle also relates to the owner of the vehicle in such a specific way that the task is to be regarded as personal data. The Government does not consider that there is now any reason to make a different assessment.

In the literature, Öman states that vehicle registration numbers are examples of information relating to an identifiable natural person.⁸

Right of access without undue delay

The controller is obliged to provide any person who so requests with information on the processing or non-processing of personal data relating to the applicant. Processing such data shall, in accordance with Article 15 of the GDPR, provide the complainant with additional information as well as a copy of the personal data processed by the controller.

According to Article 12(3) GDPR, the controller shall upon request without undue delay and in any event no later than one month after receiving the request for access and respond to the data subject's request.⁹

Assessment of the Swedish Authority for Privacy Protection (IMY)

On the basis of the complaint in the case, IMY only examined the company's conduct in the individual case and whether it provided a copy of the personal data relating to

⁵ Prop. 2013/14:25 p. 85.

⁶ Prop. 2000/01:95 p. 98.

⁷ Prop. 2003/04:145 pp. 98 et seq.

⁸ Öman, S. Data Protection Regulation (GDPR) etc. 2, the commentary on Article 5, under the heading "First paragraph — Personal data".

⁹ European Data Protection Board Guidelines 01/2022 on data subjects' rights — right of access, version 1.0, adopted on 18 January 2022.

the complainant without undue delay. Supervision does not apply if the company's personal data processing is otherwise compatible with the General Data Protection Regulation (GDPR).

The IMY considers that the information requested by the complainant on technical records and data from the vehicle guarantee, constitute personal data relating to the applicant, since they relate specifically to the applicant as the owner of the vehicle and may be used to identify the complainant.¹⁰ In so doing, the complainant is entitled to access the data from the company upon request in accordance with Article 15 of the GDPR, *inter alia*, the information set out in Article 15(1) and a copy of the data pursuant to Article 15(3).

The complainant has stated that the request for access was made in March 2019. On the other hand, the company has states that the applicant's request for access was made only on 25 February 2020. IMY finds no reason to question the company's statements that the applicant's request was received by the company on 25 February 2020. However, IMY considers that this request was sufficiently clear and clear to refer to all personal data relating to the complainant's vehicles, including the above-mentioned data which the company made available to the applicant only on 15 September 2021. This is because the complainant indicated in its request the type of information about his vehicle for which the complainant requested data and that the controller should assume that, in the event of a request for access, the data subject intends to exercise his or her full right pursuant Article 15(1) to (2) of the GDPR.¹¹ The request has thus been met 17 months after the external deadline of one month for: to deal with the request in accordance with the general rule in Article 12(3). IMY therefore considers that Volvo Personvagnar AB has not dealt with the complainant's request for access pursuant Article 15(3) without undue delay within the meaning of Article 12(3) of the GDPR.

The fact that most of the information was disclosed earlier and that the company stated that the error was attributable to the human factor, does not cause any other assessment.

In the light of the above, IMY concludes that Volvo Personvagnar has processed the complainant's personal data in violation of Article 12(3) of the GDPR by not responding without undue delay to the complainant's request of 25 February 2020 for access pursuant Article 15(3) only on 15 September 2021.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine.

In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is

¹⁰ Cf. EDPB Opinion 01/2020 on Connected Vehicles, paragraphs 3, 29 and 62.

¹¹ Cf. EDPB Guidelines 01/2022 on data subjects' rights — right of access, version 1.0, adopted on 18 January 2022, paragraph 51.

the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The infringement has affected one person and the company has reviewed its procedures. The company essentially satisfied the complainant's right of access without undue delay and has now also granted the complainant access to all his personal data. The Company has not received any corrective action for breach of GDPR. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Volvo Personvagnar AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been approved by the specially appointed decision-maker [REDACTED]

[REDACTED] after presentation by legal advisor [REDACTED]

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision, no. DI-2021-10448. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-10448, IMI case no.
350245,
83.41/20.039

Decision under the General Data Protection Regulation – Klarna Bank AB

Date of decision:
2022-06-14

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that Klarna Bank AB has processed personal data in breach of Article 15 of the GDPR¹ by not giving the complainant access to his personal data without undue delay, according to the request of 15 October 2020, until 21 January 2022.

The Swedish Authority for Privacy Protection issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) GDPR for violation of Article 15.

Report on the supervisory case

The case handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as lead supervisory authority under Article 56 of the GDPR. The handover has been made by the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the GDPR's provisions on cooperation concerning cross-border processing.

The investigation in the case has been carried out through written correspondence. Since this is a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned has been the data protection authorities in Denmark, Finland, Germany, France, Norway and the Netherlands.

The complaint

The complaint mainly states the following.

The complainant used Klarna's services for an internet purchase several years ago. The complainant's partner then received bills which in some cases were addressed to

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

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).

the complainant. In December 2018, the complainant requested Klarna to correct the names in the e-mails. Klarna's services were not used again until 2020 by the complainant's partner, after which the complainant's partner once again received e-mails from Klarna with the complainant's name. The complainant subsequently made a request for rectification. The complainant also submitted a request for access on 15 October 2020 but received no reply from Klarna.

What Klarna has stated

Klarna Bank AB mainly states the following.

Klarna is the data controller for the processing to which the complaint relates.

Klarna notes that the complainant has made three purchases in 2017 and 2018 and paid through Klarna. Those purchases included information about the complainant's first name, surname and postal address, as well as an e-mail address containing the complainant's name. In 2018, a further five purchases were made in which the complainant's first name, surname and postal address were entered. On these purchases, another e-mail address was entered, hereinafter referred to as "e-mail address Y".

Klarna notes that the complainant's partner lives at the same postal address as the complainant. The complainant's partner has also paid with Klarna on several occasions and has entered "e-mail address Y" for each purchase. Klarna suspects that the email address in question belongs to the complainant's partner because it contains the partner's name.

For each purchase, Klarna evaluated the identity of the complainant on the basis of the information provided at the time of purchase, i.e. first name, surname and postal address, by validating the data with the support of Deutsche Post AG. However, e-mail addresses are not part of the validation as it is not a data point available to Deutsche Post AG. Deutsche Post AG has thus verified that the first and last names of the complainant are registered at the provided postal address, which is also the address to which the purchased goods have been sent. Digital communication about purchases and debts is sent to the e-mail address provided by the customer.

Regarding the five purchases in 2018, the orders have been made with the complainant's first name, surname, postal address and "e-mail address Y". This is information that has been submitted to Klarna in connection with the purchases. This can be done by entering the complainant's name at the merchant's login portal and saved with the merchant as part of the customer's profile. The information is then automatically sent to Klarna when the customer is logged in with the merchant and places an order. This can also be done if the data has been entered manually in a free text field in the merchant's checkout provided by Klarna. This handling is outside Klarna's control and the company has no access to any information about this. Klarna can only state that the information has been sent to Klarna in one of the ways above.

For all five purchases in 2018, for which the complainant has claimed that the complainant's partner made the purchases, the complainant's first name, surname and postal address have been entered together with "e-mail address Y". As a result, the first e-mail sent to "email address Y" has included the complainant's name. In the context of a subsequent sixth purchase on 31 August 2020, the information that Klarna had previously linked to "email address Y" was used to generate a first name in an e-

mail of 22 September 2020 using the complainant's first name in the introductory greeting. No personal data other than the complainant's first name were sent out.

Klarna has had extensive contact with the complainant on a number of subjects. As can be seen from the notes that Klarna still retains, the complainant has requested that information be rectified on two occasions, on 5 November 2018 and on 10 October 2020. Klarna has rectified all the information which the complainant has requested to be corrected.

In examining the case, Klarna also understood that the complainant and their partner used each other's personal data for purchases carried out in 2018, which were not covered by the complainant's requests for rectification. Klarna has been able to conclude from the review that the name for individual historical purchases has had to be updated.

Klarna has received a request for access on 15 October 2020. In the light of previous extensive contacts with the complainant and the request for rectification already pending since 10 October 2020, the individual case handler did not draw attention to the fact that the request of 15 October 2020 related to a different right. The case handler was under the impression that the complainant's request for access would be handled in the context of the pre-existing case.

The correct procedure under Klarna's internal routines would have been to initiate an additional case concerning the request for access. Klarna observes that, as a result of that individual error, the complainant's request was not handled within the time limit. Following IMY's audit, Klarna has carefully analysed the case, drawing attention to the request for access and fulfilling it on 21 January 2022.

Justification of the decision

Applicable provisions

According to Article 4(1) of the GDPR, the term 'personal data' carries broad meaning. Personal data are any information relating to an identified or identifiable natural person (a data subject). A data subject can be identified both directly and indirectly by a range of possible identifiers, which the article contains a non-exhaustive list of, including names.

Article 5(1)(d) of the GDPR requires the controller to ensure that personal data is processed is accurate (principle of accuracy). If necessary, the personal data shall also be kept up to date. The controller must of its own volition take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Pursuant to Article 15 of the GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. If such personal data are processed, the controller shall provide the data subject with additional information and a copy of the personal data processed by the controller.

Pursuant to Article 16 of the GDPR, the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data

subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 12(3) of the GDPR requires the controller to provide information on action taken on a request under, inter alia Article 15, without undue delay and in any event within one month of receipt of the request. This period may be extended by a further two months where necessary, taking into account the complexity and number of requests. The controller shall inform the data subject of such extension within one month of receipt of the request, together with the reasons for the delay.

Assessment by the Integrity Protection Authority

Has there been a breach of Article 5 of the GDPR?

The complaint states that Klarna has regularly confused the personal data of the complainant and their partner by addressing several e-mails to the wrong recipient.

Among other things, Klarna has stated that they have a system for automatic generation of first names in the initial greeting of e-mails. Both the complainant and their partner have used the same e-mail address, i.e. "e-mail address Y". The complainant's partner has previously placed orders with their corresponding personal data and "e-mail address Y". In connection with a sixth purchase in 2020, Klarna has used the latest known information about "e-mail address Y", which resulted in the complainant's first name being generated in an initial greeting in the e-mail message. IMY has found no reason to question Klarna's information in this regard.

IMY therefore notes that "e-mail address Y" has been used by both the complainant and the complainant's partner to pay through Klarna. Although IMY considers it important that a correct first name is used when a data controller contacts a data subject, "email address Y" has been used by both the complainant and their partner to place orders through Klarna in the present case. No other personal data than the complainant's first name has been entered in the e-mail message to their partner, and it also appears that the complainant's first name is relatively common. The name in question does therefore not constitute an identifier specific to the complainant. Moreover, Klarna has of its own volition rectified information attributable to the complainant, which was not covered by any of the complainant's requests.

Against this background, IMY notes that the investigation does not show that Klarna Bank AB fails to comply with Article 5(1)(d) GDPR in the matter that is subject to supervision in the present case.

Has there been a breach of Article 16 of the GDPR?

Klarna states that they have received two requests for rectification from the complainant on 5 November 2018 and 10 October 2020. Klarna has stated that it has rectified all the information per the complainant's requests without undue delay. The complainant has not claimed that their requests for rectification were not met to any extent. IMY therefore finds no reason to question Klarna's information in this regard.

IMY therefore concludes that the investigation shows that Klarna Bank AB does not fail to comply with Article 16 of the GDPR in the matter that is subject to supervision in the present case.

Has there been a breach of Article 15 of the GDPR?

Klarna has stated that they received a request for access on 15 October 2020. Due to an error, the company did not recognize the request at that time. The request was brought to Klarna's attention after IMY initiated its audit and was therefore only completed on 21 January 2022, i.e. approximately one year and three months after the request was made.

A request for access shall be handled without undue delay, but no later than within one month from when the controller received the request. The deadline of one month may be extended by a further two months under the conditions set out in Article 12.3 GDPR. Considering Klarna fulfilled the complainant's request for access more than one year after the request was made, it is clear that Klarna under no circumstances handled the complainant's request within any of the deadlines set out in the GDPR. Klarna's explanation to the reason for the delay being an oversight by a case handler does not change IMY:s assessment. Therefore, Klarna did not handle the complainant's request for access of 15 October 2020 without undue delay.

IMY therefore concludes that Klarna Bank AB has infringed Article 15 GDPR by not giving the complainant access to their personal data without undue delay, according to their request of 15 October 2020, until 21 January 2022.

Choice of intervention

Article 58(2) and Article 83(2) of the GDPR gives IMY the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as warnings and prohibitions. Furthermore, it is clear from Article 83(2) which factors are to be taken into account when deciding whether to impose administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may issue a reprimand pursuant to Article 58(2)(b) instead of imposing a fine. Considering the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. Klarna has infringed Article 15 of the GDPR by not handling the complainant's request for access without undue delay. The time that has elapsed since the request for access was made is relatively long. As is made clear by the supporting documents, the complainant has made several requests, including a request for rectification on 10 October 2020 and a request for access on 15 October 2020, after which a case handled at Klarna had not understood that they were different rights. It is therefore a mistake. In light of this, IMY considers that this is a minor infringement within the meaning of recital 148 which means that Klarna Bank AB shall be given a reprimand under Article 58(2)(b) of the GDPR for the infringement.

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED] following a presentation by [REDACTED]

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision, no. DI-2021-10665. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-10665, IMI case no.
351839,
521.15317_631.464

Decision under the General Data Protection Regulation – Klarna Bank AB

Date of decision:
2022-06-14

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that Klarna Bank AB has processed personal data in breach of Article 12(3) of the GDPR¹ by not informing the complainant without undue delay of the outcome of the complainant's request for erasure pursuant to Article 17 of 15 October 2021 only on 18 November 2021.

The Swedish Authority for Privacy Protection issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) GDPR for infringement of Article 12(3) of the GDPR.

Report on the supervisory case

The case handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as lead supervisory authority under Article 56 of the General Data Protection Regulation (GDPR). The handover has been made by the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the Regulation's provisions on cooperation concerning cross-border processing.

The investigation in the case has been carried out through written correspondence. Since the complaint relates to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Finland, Italy, Poland, Germany and Austria.

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

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).

The complaint

The complainant mainly states the following. A request for erasure was made to Klarna on 15 October 2021 and the complainant had not received any response from Klarna as of 16 November 2021.

What Klarna has stated

Klarna mainly states the following.

Klarna is the data controller for the processing to which the complaint relates.

Klarna received the request for erasure on 15 October 2021. Klarna initiated the erasure of the complainant's personal data on 29 October 2021 and completed it on 15 November 2021. Confirmation on the erasure of the complainant's personal data was sent to the complainant on 18 November 2021.

According to Klarna's internal procedures, a confirmation on the initiation of personal data erasure should be sent to the person requesting erasure by e-mail as soon as the erasure process is initiated, in this case on 29 October 2021. In the present case, no such confirmation e-mail was sent until the 18 November 2021. However, this has not affected the actual deletion of the complainant's personal data.

Justification of the decision

Applicable provisions

Article 17(1)(a) states 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, if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Article 17(3) lists all exceptions to this right.

Article 12(3) of the GDPR requires the controller to provide information on action taken on a request under, inter alia Article 17, without undue delay and in any event within one month of receipt of the request. This period may be extended by a further two months where necessary, taking into account the complexity and number of requests. The controller shall inform the data subject of such extension within one month of receipt of the request, together with the reasons for the delay.

IMY:s assessment

Klarna states that the complainant's request for deletion was received by Klarna on 15 October 2021 and that the data had been deleted on 15 November 2021. IMY finds no reason to call this into question. IMY therefore considers that the request for erasure has been carried out without undue delay.

Article 12(3) also imposes an obligation for the controller to provide information on the action taken in response to the request. Such information shall be provided without undue delay and in any event no later than one month after the controller receives the request.

Klarna informed the complainant on 18 November 2021, i.e. three days later than one month after Klarna had received the request. Although the time frame of one month may be extended under certain circumstances in accordance with Article 12(3), it is

required that the controller notifies the data subject of such a delay and the reason for the delay within one month from when they received the request. It has not been established that Klarna provided the complainant such notification. IMY therefore finds that Klarna has processed personal data in breach of Article 12(3) by not informing the complainant of the outcome of their request for erasure without undue delay.

Choice of intervention

Article 58(2) and Article 83(2) of the GDPR gives IMY the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to, or in place of the other measures referred to in Article 58(2), such as warnings and prohibitions. Furthermore, it is clear from Article 83(2) which factors are to be taken into account when deciding whether to impose administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may issue a reprimand pursuant to Article 58(2)(b) instead of imposing a fine. Considering the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The infringement has affected one person, lasted a relatively short period of time and occurred as a result of a mistake. In light of this, IMY considers that this is a minor infringement within the meaning of recital 148 which means that Klarna Bank AB shall be given a reprimand under Article 58(2)(b) of the GDPR for the infringement.

This decision has been approved by the specially appointed decision-maker, legal advisor [REDACTED] following a presentation by legal advisor [REDACTED]

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-06-27, no. DI-2020-10696. Only the Swedish version of the decision is deemed authentic.

Ref no:
2020-10696,
IMI case no. 134903

Date of decision:
2022-06-27

Date of translation:
2022-06-27

Decision under the General Data Protection Regulation – Nordax Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Nordax Bank AB has processed personal data in breach of:

- Article 15 of the General Data Protection Regulation (GDPR)¹ by failing to handle the complainant's requests of access made on 5 December 2018 and 11 February 2019.
- Article 17 by not without undue delay handle the complainant's requests for erasure made on 5 December 2018 and 11 February 2019.
- Article 12(3) by not without undue delay provide information to the complainant on the measures taken, namely that the complainant was blocked from direct marketing mailings, in response to the complainant's objection to direct marketing made on 9 July 2019.

The Swedish Authority for Privacy Protection finds that Nordax Bank AB has processed personal data in breach of:

- Article 12(6) by requesting the complainant to submit further information in order to comply with the request to object to direct marketing on 9 July 2019, even though the data provided in the request was sufficient to actually complete the request.

The Authority for Privacy Protection issues Nordax Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of the Articles 12(3), 12(6), 15, 17 of the GDPR.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

In accordance with Article 58(2)(c) of the GDPR, IMY orders Nordax Bank AB to:

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).

- Comply with the complainant's request to exercise its right of access under Article 15 of the GDPR, with exception for information which is subject to any applicable derogation provided for in Article 15(4). This is done by providing the complainant access to all personal data that Nordax process regarding the complainant by providing the complainant with a copy of the personal data referred to in Article 15(3) and provide information pursuant to points (a) to (h) of Article 15(1) and 15.2. The measures shall be implemented no later than two weeks after this decision has become final.

In accordance with Article 58(2)(d) of the GDPR, IMY orders Nordax Bank AB to:

- Handle the complainant's request of erasure of all of his personal data according to Article 17 by assessing whether there is personal data that the company in accordance with Article 17 is obliged to erase and, if so, to do so, and to inform the complainant in accordance with Article 12(3) or (4). The measures must be implemented no later than two weeks after this decision has become final.

In accordance with Article 58(2)(d) of the GDPR, IMY orders Nordax Bank AB to:

- In accordance with Article 12(3), provide the complainant with information on the measures which have been taken in response to the complainant's request to exercise his right of objection to processing for direct marketing purposes. The measures shall be implemented no later than two weeks after this decision has become final.

Report on the supervisory matter

The Authority for Privacy Protection (IMY) has initiated supervision regarding Nordax Bank AB (Nordax or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Norway) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, Denmark, Finland and Germany.

The complaint

The complaint states the following. The complaint alleges that the company has not dealt with the complainant's requests to exercise the complainant's rights under the GDPR in relation to the right of access pursuant to Article 15, the right of erasure pursuant to Article 17 and objection to obtaining personal data processed for direct marketing purposes as referred to in Article 21(2). E-mail correspondence with the company is attached to the complaint.

What Nordax has stated

Nordax has mainly stated the following.

Nordax is the data controller for the processing to which the complaint relates. The processing is carried out by Nordax personal data processor Iper Direkt AB (Iper) on behalf of Nordax and for direct marketing purposes, which is regulated in agreements between Nordax and Iper. Nordax determines the purposes and means of the processing. The relationship can be compared to the example set out in the EDPB Guidelines 07/2020 on the terms "controller" and "processor" in GDPR, ("Example: market research").²

Iper is responsible and the controller of the address register and responsible for managing the rights of data subjects whose personal data are available in this address register. Based on these, Iper makes, on behalf of Nordax, a selection from its address register and provides the addresses to another data processor that Nordax uses to carry out the marketing mailings. Nordax does not process or store any personal data since the data provided by Iper to Nordax is de-identified.

Right of access

Nordax Bank AB originally received a request for access from the complainant on 5 December 2018. The request concerned "information on all data relating to me as you have stored and what the data is used for". The complainant's request was answered by email on 6 December 2018 with the information that the complainant's personal data are not processed by Nordax why a request for access (or erasure) could not be handled. Nordax states that, as a data controller, however, the company should have interpreted this as a request under Article 15 of the GDPR and provided the complainant with access to personal data with the help of the personal data processor Iper in accordance with the provisions of Article 28 of the GDPR. Nordax took the view that the complainant's main request was not a request of access to personal data pursuant to Article 15. In the light of the information in the complainant's email and that the complainant did not contact Nordax after a block on direct marketing was established in respect of the complainant on 9 July 2019, Nordax considered that the complainant's primary wish was to be blocked against addressed direct marketing from the company. Nordax believes that the complainant considers that the request for objection has been dealt with but can definitely comply with the complainant's request for access if the complainant still wishes to exercise its right to access to the personal data.

Right to erasure

The complainant's request for erasure was received on 5 December 2018 and Nordax replied to it on 6 December 2018. It was clear from the reply that the company did not consider that it stored the complainant's personal data, why any erasure of data at Nordax could not be done. It is the address provider Iper, Nordax data processor, who is reported to have stored the complainant's personal data at the time of the complainant's request. Iper is controller of the address register for which Nordax receives addresses for direct marketing mailings. Nordax does not have the ability to erase personal data in Iper's register. It is against this background that Nordax has not complied with the complainant's request for erasure.

Furthermore, Nordax states that the company is currently processing personal data regarding the complainant in order to maintain a block on addressed direct marketing, which is necessary to comply with a legal obligation. Nordax has by e-mail on 6 December 2018 and 16 July 2019 provided general information to the complainant that Nordax may process the complainant's personal data in order to maintain a block on addressed direct marketing. Personal data of the complainant is also being processed to deal with the ongoing supervisory case which will be discontinued when the enforcement case is closed. The company has not interpreted the complainant's

² EDPB 07/2020 on the concepts of controller and processor in the GDPR, 2,0, page 19.

request for erasure in such a way that it would have included these ongoing processes of personal data.

Right of objection

The complainant submitted a request for access and deletion on 5 December 2018 which Nordax replied on 6 December 2018. In the light of the information in the complainant's request Nordax presumed that the complainant had received addressed direct marketing mailings of Nordax products. Therefore, Nordax provided information on how the complainant should proceed with a block against further direct marketing mailings of Nordax products. In order to block an individual against addressed direct marketing Nordax needs information about the individual's pre- and surname and full address which the company informed the complainant about. Nordax never received additional information from the complainant and could not therefore block the complainant from the addressed direct marketing mailings. On 11 February 2019, the complainant submitted a further request for access and erasure and objection to receiving direct marketing mailings. Nordax responded to the complainant's request on 12 February 2019 by referring to an earlier reply to the request for access and erasure and stated that Nordax has granted the complainant's request to object to receiving further direct marketing. However, the complainant was wrongly informed on that occasion that Nordax had taken measures to prevent the complainant from receiving further direct marketing mailings. Nordax believes that the handling of the case in question has failed due to the human factor and the company reviews its procedures for individuals who wish to object to direct marketing mailings because of this, to ensure that incorrect information is not sent again.

The complainant's lodged a further complaint on 9 July 2019, which Nordax once again replied with information on how the complainant should proceed in order to block himself against addressed direct marketing mailings. At the time of receipt of this objection, the complainant was also finally blocked against further addressed direct marketing mailing from Nordax products. However, Nordax has not informed that complainant was blocked from such further direct marketing mailings of Nordax products. Nor did the complainant contact Nordax after 9 July 2019.

Justification of the decision

Applicable provisions, etc.

Data controller

The controller, as defined in Article 4(7) of the GDPR, means the natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data.

In the European Data Protection Board (EDPB) Guidelines 07/2020 on the concepts data controller and processor in the General Data Protection Regulation the following is mentioned concerning the respective roles of processors and controllers in the exercise of data subjects' rights:

"It is crucial to bear in mind that, although the practical management of

individual requests can be outsourced to the processor, the controller bears the responsibility for complying with such requests. Therefore, the assessment as to whether requests by data subjects are admissible and/or the requirements set by the GDPR are met should be performed by the controller, either on a case-by-case basis or through clear instructions provided to the processor in the contract before the start of the processing. Also, the deadlines set out by Chapter III cannot be extended by the controller based on the fact that the necessary information must be provided by the processor.”³

It also states the following in an example, to which Nordax refers to concerning the relationship between Nordax and Iper:

“Example: Market research 1 Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information. Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research. Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself. Nevertheless, Company ABC decided that the processing should take place, the processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.”⁴

In the literature, Öman points out the following.

“The legal person which engages any other legal person to process personal data, e.g. for storing and disseminating or for collecting and processing the personal data, is normally considered to be the data controller and the hired as a personal data processor. This applies even if it is the hired company and not the company who hires who has the knowledge of how to best process the personal data, such as how to store, collect, disseminate and process them, and the resources to do it. In fact, the company who hires has decided the means of processing of the personal data by employing a company that can use certain methods. This may involve outsourcing IT operations or to hire a company to collect personal data within the framework of a market research.”

Rights of the data subject

According to Article 12(3) of the GDPR, the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Pursuant to Article 12(6), where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

³ EDPB 07/2020 on the concepts of controller and processor in the GDPR, 2.0, paragraph 132.

⁴ EDPB 07/2020 on the concepts of controller and processor in the GDPR, 2.0, page 19.

Under Article 15(1), the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data from the controller.

Pursuant to Article 17(1), 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 under certain conditions set out in the current article.

Under Article 21(2) and (3), the data subject shall have the right to object at any time to processing of personal data for direct marketing purposes concerning him or her. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Assessment of the Authority for Privacy Protection (IMY)

On the basis of the complaint in this case, IMY examined the company's conduct in the individual case. Therefore IMY will not consider whether the company's current procedure for processing requests is compatible with the GDPR, but may take into account possible improvements when considering choice of corrective measures.

Is Nordax's data controller for the processing in question and has the company been obliged to deal with the complainant's requests to exercise his rights?

The question in this case is whether Nordax has had an obligation to comply with the complainant's requests for access, erasure and objection under the GDPR and in that case, if the company handled the complainant's requests correctly. In order to investigate this, IMY first needs to consider whether Nordax is the controller of personal data for the processing of personal data in this case.

Nordax has stated that the company is the data controller for the processing. The processing consists of the fact that the company Iper — on behalf of Nordax and based on selection criteria that Nordax determines — makes a selection from Iper's address register and provides addresses for the sending of direct marketing to a third company that Nordax hires to make the mailings. Nordax argues that the company itself does not deal with any data, as the data provided by Iper to Nordax are de-identified.

The investigation shows that Nordax initially failed to comply with the complainant's first requests for access and erasure pursuant to Articles 15 and 17 on the grounds that the Company does not process or store the complainant's personal data and that instead the complainant should refer directly to Iper. IMY notes, however, that it is not required to have access to or store personal data in order to be considered to be data controller for a particular processing operation. What matters is who decides the purposes and means of the processing.

Since the processing consisting of the selection from Iper's address register for direct marketing is carried out on behalf of Nordax and based on the selection criteria that Nordax has decided, IMY believes that Nordax determines the purpose and means of the processing and is therefore the controller for the processing. This means that Nordax is responsible for handling the complainant's requests, either by handling the request itself or to give clear instructions to for example a data processor, in order for

the data processor to be able to do so.⁵ Nordax's argument that it is not responsible for Iper's address register does not alter that.

What Nordax has stated that Nordax receives only de-identified data from Iper is irrelevant for the company's responsibility to deal with the complainant's requests. Nordax is responsible for the processing of personal data carried out by Iper namely the selection of the advertising received by the complainant to which the complaint relates.

There is therefore no need to consider whether the data received by Nordax are de-identified in such a way that they are not personal data. IMY points out that even information that can directly or indirectly identify a natural person is personal data, including information that has been encoded, encrypted or pseudonymised but which can be linked to a natural person with help of additional information.

Since IMY has found that Nordax is the data controller for the processing that the complaint concerns and is therefore responsible for ensuring that the complainant's requests to exercise its rights under the GDPR are dealt with, IMY goes on to investigate whether Nordax handled the requests correctly under the Regulation.

Has Nordax handled the complainant's requests to exercise its rights been in compliance with the GDPR?

Request for access

It is apparent from the investigation that the complainant submitted its first request to access to the company on 5 December 2018. The request was worded in such a way that the complainant would like to receive access to all data stored by the company on the complainant and information about what the data was used for. Nordax did not take any action other than to inform the complainant that the complainant's personal data were not being processed by the company and that the request could therefore not be met. At the same time, Nordax informed of its process for selection and dispatch of addressed direct marketing and which address provider Nordax uses for selection of addresses. The complainant subsequently submitted its second request for access on 11 February 2019, to which Nordax replied on 12 February by referring to its previous reply to the complainant.

During the investigation Nordax stated that it should have interpreted the complainant's requests as a request to exercise their right of access under Article 15 of the GDPR and provided the complainant with the data and information to which the complainant was entitled too with the assistance of Iper. IMY shares this assessment. IMY notes in that regard that it is true that, in its request, the complainant referred to the storage data, but that nevertheless, it should have been clear to Nordax that the complainant intended to exercise its full right of access and that it is Nordax responsibility, such as data controller for the processing, to ensure that the request was handled.

Furthermore, IMY notes that Nordax has still not complied with the request even though the company now admits that the company is obliged to do so. Nordax has stated that it can comply with the complainant's request for access if the complainant so wishes. IMY notes, however, that there has been no evidence to suggest that the request still wouldn't be relevant, such as the fact that the complainant would have

⁵ EDPB 07/2020 on the concepts of controller and processor in the GDPR, 2.0, paragraph 132.

withdrawn it. By failing to comply with the applicant's request for access Nordax has processed personal data in violation of Article 15 of the GDPR.

Request for deletion

It is apparent from the investigation that, on 5 December 2018, the complainant also submitted his first request for deletion. Nordax did not take any action other than to inform the complainant that the complainant's personal data were not processed by the company and that the request could therefore not be met. At the same time, Nordax informed of its process for selection and dispatch of addressed direct marketing and which address provider Nordax uses for selection of addresses. The complainant subsequently submitted its second request for deletion on 11 February 2019, to which Nordax replied on 12 February by referring to its previous reply to the complainant.

Article 17(3) of the GDPR provides for an exhaustive demonstration of the grounds on which a request for erasure may be rejected. That the controller not storing the data being processed is not such a basis. As IMY has stated above, the company is obliged to deal with the complainant's requests, which the company haven't done. Nordax thus processes personal data in violation of Article 17 of the GDPR by not without undue delay handle the complainant's requests for erasure.

Request for objection

The investigation shows that Nordax perceived that, on 5 December 2018, the complainant also submitted an objection to the processing of personal data for direct marketing purposes pursuant to Article 21(2) GDPR. Nordax informed the complainant how the complainant could proceed to object to further direct marketing and requested additional information from the complainant in order to be able to fulfil that right. However, the complainant did not return with additional information.

IMY considers that, as the request was worded, the complainant had not invoked its right of objecting to direct marketing. IMY therefore notes that Nordax did not have any obligation to deal with it as such a request, but welcomes the fact that Nordax nevertheless provided information on how the complainant could proceed to block further direct marketing.

However, the complainant lodged its first actual request of objection to further direct marketing on 11 February 2019. Nordax provided information that the complainant had been blocked against further direct marketing, but the information at this point was incorrect. Because Nordax left incorrect information to the complainant on 12 February 2019 on the measures taken on the basis of the complainant's request for objection meaning that the complainant's information was blocked for further direct marketing mailings Nordax has acted in violation of article 12.3.

The complainant lodged its second objection on 9 July 2019. Nordax replied to the complainant on 16 July 2019 referring to previous replies on how the complainant could try to block him or herself from further marketing. The company however blocked, the complainant against further addressed direct marketing on 9 July 2019, but did not inform the complainant of this measure.

Against this background, IMY takes the view that Nordax has satisfied the complainant's second request of objection pursuant to Article 21(2) of the GDPR.

In Nordax reply to the second request, the company asked the complainant to submit additional information in order to comply with the request, even though the existing information in the request according to Nordax, was sufficient to actually satisfy the request directly. For this reason Nordax has requested additional information that has not been necessary to confirm the identity of the data subject in violation of 12(6).

Furthermore, Nordax did not inform the complainant that, in accordance with its second requests for objection the complainant was blocked against further addressed direct marketing. By doing so, Nordax has failed to fulfil its obligation under Article 12(3) to provide the data subject with information on the measures taken under Article 21 and thus processed personal data in breach of Article 12(3) of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. Nordax have stated that they have taken action by reviewing their procedures to ensure that incorrect information should not be sent again and reviewing how the company handles data subjects' rights regarding processing carried out on the company's behalf by the company's processor. According to IMY the noted infringements found occurred relatively far back in time, partly due to the human factor and has affected one person. In addition, the company has not previously acted in breach of the GDPR.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Nordax Bank AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

Since the company has not handled the complainat's request for access even though the company is obliged to do so, IMY considers that there is reason in accordance with Article 58(2)(c) to order the company to comply with the complainant's request to exercise its right of access under Article 15 with exception for information which is subject to any applicable derogation provided for in Article 15(4). This is done by providing the complainant access to all personal data that Nordax process regarding the complainant by arranging a copy to the complainant of the personal data referred to in Article 15(3) and provide information pursuant to points (a) to (h) of Article 15(1) and 15.2. The measures shall be implemented no later than two weeks after this decision has become final.

The company has also failed to deal with the complainant's request for erasure even though the company is obliged to do so. IMY therefore considers that it is appropriate, on the basis of Article 58.2(d) to order the company to deal with the complainant's request for erasure of all personal data referred to in Article 17 by considering whether

there is personal data which the company is obliged to erase in accordance with Article 17 and, if so, erase the information and inform the complainant in accordance with Article 12(3) or (4). Measures shall be completed no later than two weeks after the date on which this decision has become final.

Furthermore, Nordax did not inform the complainant about the measure which been taken, namely that the complainant been blocked for further addressed direct marketing, in response to the complainant's second request to exercise the right of objection to process for direct marketing purposes. IMY considers that it is appropriate, pursuant to Article 58(2)(d), to order the company to in accordance with Article 12(3), provide the complainant with information on the measures which been taken in response to the complainant's request to exercise his right of objection to processing for direct marketing purposes. The measures shall be implemented no later than two weeks after this decision has become final.

This decision has been approved by the specially appointed decision-maker [REDACTED]

[REDACTED] after presentation by legal advisor [REDACTED]

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-07-20, no. DI-2022-1687. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2022-1687, IMI case no.
155158

Date of decision:
2022-07-20

Date of translation:
2022-07-20

Final decision under the General Data Protection Regulation – If Skadeförsäkring AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that If Skadeförsäkring AB has processed personal data in breach of:

- Article 12(3) of the General Data Protection Regulation (GDPR)¹ by not, without undue delay, handle the complainant's request of access under Article 15 in accordance with the complainant's request of 31 October 2018.
- Article 15 by not giving the complainant additional information on the processing pursuant to Article 15(1) and 15(2) of the GDPR when the complainant received a copy of a transcribed telephone call on 26 February 2019.

The Authority for Privacy Protection issues If Skadeförsäkring AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(3) and 15 of the GDPR.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding If Skadeförsäkring AB (If Skadeförsäkring or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the GDPR. The handover was made from the supervisory authority of the country where the complainant has lodged their complaint (Norway) in accordance with the Regulation's provisions on cooperation in cross-border processing.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory

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).

authorities concerned have been the data protection authorities in Finland and Norway.

The complaint

The complaint states the following. On 31 October 2018, the complainant contacted the company and requested to obtain a copy of all the documentation relating to two leak damages in the residential property in which the complainant have their apartment. The water damage was reported to have been caused by the complainant's apartment. In addition, the complainant requested access to a recorded telephone call between the complainant itself and the company from 5 October 2018.

On 7 December 2018, the complainant received a reply from the company and only obtained documentation relating to the damage from 2013 but not the damage from 2015.

The complainant and the company had further contact via telephone and e-mail during December 2018 and January 2019. On 22 February 2019, the complainant contacted the company again by telephone and made clear that they wished to have access to documentation relating to the water leak from 2015. On 25 February, the complainant reminded the company by e-mail of what had been agreed during the last telephone call. On 26 February, the complainant received an e-mail from the company containing parts of the telephone conversation in a transcribed form. However, the transcription was full of spelling errors, which made it impossible to understand what was said. The e-mail contained no documents relating to the water leak from 2015.

What If Skadeförsäkring has stated

If Skadeförsäkring has mainly stated the following. If Skadeförsäkring is the data controller for the processing to which the complaint relates through its Norwegian branch If Skadeforsikring NUF, which has organisation number 981 290 666 in the Norwegian Business Register. If Skadeförsäkring's branches in Finland, Denmark and Norway do not have their own national management and operations are governed by the Nordic organisation.

On 31 October 2018 the complainant requested to get access to all documentation relating to the complainant's apartment that was linked to the water damages. The complainant also requested a recording of a telephone call between the complainant and a damage adviser on 5 October 2018.

It is the condominium association in which the complainant lives, that is the policyholder (insured) and that in 2013 and 2015 reported damages regarding water leakage in the association. The insurance claim from 2013 contains information related the complainant, while the 2015 insurance claim does not contain any information that can be linked to the complainant.

The company did not perceive the complainant's request of 31 October 2018 for access to documentation relating to the water leak and the complainant's apartment as a request under Article 15 of the GDPR. The complainant submitted the request by e-mailing the company's Norwegian property damage department.

On 7 December 2018 the company informed the complainant that he has the right to access only documents relating to him or her. Documents containing information which may be linked to the complainant were enclosed in the e-mail. The complainant received a transcript of the recorded call on 26 February 2019. The reason why it took

until 26 February 2019 before the complainant received the transcription is that the company did not perceive the complainant's request as a request for access under Article 15 of the GDPR and therefore did not handle it according to the company's privacy practices. The case was submitted on 27 November 2018 to the department dealing with requests for access to telephone calls. One factor that further contributed to the delay was that it was a long conversation to transcribe.

If the complainant was dissatisfied with the transcript, it was possible to visit one of the company's offices to listen to the recording. Nowadays, data subjects can also receive access to recorded phone calls via a web-based solution.

In view of the way in which the complainant formulated its request, to obtain documentation on the damages and a recorded telephone call, together with the complainant's choice of communication channel, the company also did not perceive the complainant's request as a request for access to additional information under Article 15 of the GDPR. No such information was therefore provided. The company also notes that the complainant, in their complaint to the Norwegian Data Protection Authority did not mention the that absence of additional information under Article 15 constituted a deficiency in the company's handling of the complainant's request.

Justification of the decision

Applicable provisions

To anyone who requests a data controller is obliged to provide information about whether or not their personal data is being processed. If such data is processed, the controller shall, in accordance with Article 15 of the General Data Protection Regulation, provide the data subject with supplementary information and a copy of the personal data processed by the controller. It follows from Article 15(1) and (2) what additional information is to be provided to the data subject. Article 15(3) requires the controller to provide the data subject with a copy of the personal data being processed.

EDPB Guidelines 01/2022 on data subjects' rights — Right of access state:

"The obligation to provide a copy is not to be understood as an additional right of the data subject, but as modality of providing access to the data. It strengthens the right of access to the data and helps to interpret this right because it makes clear, that access to the data under Art. 15(1) comprises complete information on all data and cannot be understood as granting only a summary of the data."²

According to recital 63, the data subject should have the right of access to personal data processed in order to be aware that processing is taking place and verify the lawfulness of the processing.³

"...the purpose of the right of access is to make it possible for the data subject to understand how their personal data is being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. In other words, the purpose of the right of access is to provide the individual with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different

² Guidelines 01/2022 on data subject rights - Right of access, para 23.

³ See Judgement of 7 May 2009, Rijkeboer, C-533/07, EU:C:2009:293, paragraph 50-54.

aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).⁴

The right of access provided for in Article 15 does not constitute a broad right of access to all the documents in which a data subject's personal data are present. The purpose of the right is instead to ensure that a data subject has access to information about the processing and a copy of the personal data processed in order to be able to verify the accuracy of the data and whether they are processed in accordance with the provisions of the Regulation.⁵

According to Article 12(3), a request for access must be handled without undue delay and in any event no later than one month after the request has been received. The time limit of one month may be extended by an additional two months if the request is particularly complicated or the number of requests received is high.

If the period of one month is extended, the controller must notify the data subject of the extension. The notification of the extension of the time limit shall take place within one month of receipt of the request. The controller must also specify the reasons for the delay.

Assessment of the Authority for Privacy Protection (IMY)

Did the company have an obligation to handle the complainant's request as a request for access under Article 15 of the GDPR?

On the basis of the complaint at hand, IMY has to decide whether the company should have understood the complainant's request as a request for access under Article 15 of the GDPR and whether it in such case handled the request in accordance with the provisions of the Regulation.

The investigation has shown that the complainant contacted the company on 31 October 2018 with two requests. First, a request for access to all the documents relating to two damages on the complainant's residential property and, second, a request for access to a recorded telephone call between the complainant and an employee of the company.

The GDPR does not regulate the form in which a request for access is to be made. However, it is generally sufficient for a data subject to express their wish to obtain access to personal data processed or that they wish to have access to information about themselves held by the controller for a request to be regarded as a request for access within the meaning of Article 15.⁶

As regards the complainant's request to obtain a copy of the telephone conversation that took place between themselves and the insurance company, IMY notes that the company should have understood the complainant's request for the recorded telephone call as a request under Article 15. In particular having regard to the fact that

⁴ Guidelines 01/2022 on data subject rights - Right of access, adopted for public consultation 18 January 2022, para 10.

⁵ See the Court of Appeal Gothenburg Judgement of 2019-09-19 case no. 1677-19 and YS v. Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v. M, S, Joined Cases C-141/12 and C-372/12, European Union: Court of Justice of the European Union, 17 July 2014.

⁶ See Guidelines 01/2022 on data subject rights - Right of access, para 50.

what the complainant requested access to, the recorded call, constitutes personal data in the form of the complainant's voice recording.

As regards the complainant's request to obtain all the documentation relating to two insurance cases, IMY notes that the complainant did not state in its request that they wished to have access to personal data. The request was instead expressed as a wish to have access to all documentation relating to the damages. In view of the fact that the documents referred to by the complainant mostly contain information other than personal data and that the complainant has not stated that the request relates to access to personal data, IMY considers that it cannot be perceived as a request for access to personal data. The company has therefore not been required to deal with the complainant's request for access to all documentation in the insurance case as a request for access under Article 15.

Has the company handled the complainant's request for access without undue delay?

Since the complainant's request for access to the recorded telephone call above was found to be a request for access under Article 15 of the GDPR, IMY has to consider whether the company handled the complainant's request and whether it was done without undue delay.

The complainant submitted its request by e-mail to the company on 31 October 2018. The company provided the recorded call in transcribed form on 26 February 2019, almost four months after the complainant's request. IF Skadeförsäkring AB has therefore acted in breach of Article 12(3) by not dealing with the complainant's request for access without undue delay.

The company also states that it did not provide the complainant with additional information pursuant to Article 15(1) and (2). IMY considers that, by failing to provide the complainant with the information referred to in Article 15(1) and (2), the company failed to fulfil the complainant's request for access under Article 15. By failing to provide the additional information, IF Skadeförsäkring AB has acted in breach of Article 15.

The company's argument that the complainant did not request additional information on the processing under Article 15(1) and (2) does not change IMY's assessment. The right of access shall be regarded as one coherent right which is satisfied by the fulfilment of all elements. The company has not made sure that the complainant wished to limit their request to only a copy of the personal data pursuant to article 15(3) and that the complainant did not wish to receive the supplementary information to which the complainant was entitled.

The complainant states that the transcription received of the telephone call contained many spelling errors and was therefore impossible to understand. Regarding the fact that the company has stated that it was possible for the complainant to listen to the recorded conversation in one of the company's offices and that it is now possible for the complainant to access the recording via a web-based solution, IMY finds no reason to further examine this question

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the

circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The infringement only affected on data subject and the company partially satisfied the complainant's request for access. The company has not previously been subject to any corrective measures for infringement of data protection regulations.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that If Skadeförsäkring AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been made by the specially appointed decision-maker [REDACTED] after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision, no. DI-2021-10447. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-10447 IMI. Case no.
134712, 521.14809 / 631.420

Decision under the General Data Protection Regulation – Klarna Bank AB

Date of decision:
2022-07-28

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Klarna Bank AB has processed data in breach of

- Article 12(2) of the General Data Protection Regulation (GDPR)¹ by not facilitating the exercise of the complainant's right under Article 17 to have his data deleted in accordance with its request of 9 May 2021 because Klarna Bank AB's request for identification data was not sent out via the contact details provided by the complainant at the request.

The Swedish Authority for Privacy Protection issues Klarna Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 12(2) of the GDPR.

Report on the supervisory report

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (the company or Klarna) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR) from the supervisory authority in (Germany) where the complainant has lodged their complaint in accordance with the GDPR's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through written correspondence. Since this is a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned has been the data protection authorities in Austria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Italy, Ireland, the Netherlands, Norway, Poland and Spain.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

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).

The complaint

The complainant essentially states that, on 9 May 2021, he unsuccessfully invoked his rights pursuant Articles 17, 18, 19 and 21 of the GDPR. He further states that he has not received any information or confirmation that all of his requests have been handled.

What Klarna has stated

The company has mainly stated the following.

The company is the data controller for the processing to which the complaint relates.

The company confirms that it has received all requests by fax on 9 May 2021. On the other hand, the complainant's requests could not be met because it could not correctly identify the complainant in order to confirm that the sender of the fax is the data subject to whom the personal data relate. On 13 May 2021, the company contacted the complainant by email asking him to provide additional information to ensure identification. However, the complainant has not returned with reply. Since the complainant has not been identified, the request for erasure, restriction or objection to the processing of personal data has not been completed.

Justification of the decision

Applicable provisions, etc.

Concept of personal data

The data subject has a number of rights under Articles 15 – 22 of the General Data Protection Regulation, including the right to erasure, restriction and to object to the processing.

There is no formal requirement for making a request pursuant Article 17(1). However, Article 12(2) states that the controller shall facilitate the exercise of data subject rights under Articles 15 to 22, *inter alia*, Article 17(1).²

Pursuant to Article 17, the data subject shall have the right to have his or her personal data erased by the controller without undue delay and the controller shall be obliged to erase personal data without undue delay if they are no longer necessary for the purposes for which they have been collected or otherwise processed.

Article 12(2) requires the controller to facilitate the exercise of the data subject's rights in accordance with, *inter alia*, Article 17.

Article 12(3) provides that where the data subject makes the request by electronic form means, the information shall, where possible, be provided in electronic form, unless otherwise requested by the data subject.

Pursuant to Article 12(4), where the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy. According to recital 59 of the GDPR, controllers should, without undue delay and at the latest within one month, be required to respond to data subjects'

² See Gothenburg Administrative Court of Appeal, judgment of 30 November 2021 in Case No 2232-21, p. 3 f.

requests and to give reasons, where the controller does not intend to comply with any such requests.

It follows from Article 12(6) that where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. The way in which the identification is to be carried out is not regulated by the GDPR, but it is an assessment that the controller must make in each case. It is only if there are reasonable grounds for doubting the identity that the controller has the right to request additional information.

The European Data Protection Board (EDPB) Guidelines 01/2022 on data subject rights - Right of access, inter alia:

In cases where the controller requests the provision of additional information necessary to confirm the identity of the data subject, the controller shall each time assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate. Such additional information should not be more than the information initially needed for the verification of the data subject's identity (authentication). In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.³

Assessment of the Swedish Authority for Privacy Protection (IMY)

The investigation shows that the complaint's request was received by fax of 9 May 2021. IMY considers that at the time of the request, Klarna has reasonable doubts concerning the identity of the natural person that the sender was the data subject to whom the personal data relate or someone who had the right to act on his behalf. Klarna was therefore entitled to request further information in order to confirm this.

On 13 May 2021, Klarna attempted to request such information by sending an email to the email address previously provided by the complainant when contacting Klarna, but Klarna states that the complainant has not responded. The fact that Klarna requested additional identification data in order to confirm the identity of the complainant cannot be considered disproportionate as the data may be considered necessary to strengthen the link between the complainant and the requests.

It follows from Article 12(3) and (4) that when a data subject, or a person claiming to be a data subject, requests to exercise his or her rights, the controller is obliged to take a decision whether or not the request is complied with and to what extent and to what extent and to what extent it is communicated. If the decision is positive, i.e. compliance with the request, the controller shall inform about the measures taken (Article 12(3)). If the decision is negative, the controller shall inform the data subject of the reasons for the failure to act and of the possibility to lodge a complaint with a supervisory authority

³ European Data Protection Board Guidelines 01/2022 on data subjects' rights — right of access, version 1.0, adopted on 18 January 2022, paragraph 65..

and request a judicial remedy (Article 12(4)). This applies even if the identity of the requesting person could not be verified in accordance with Article 12(6). In order for the requesting person to be able to exercise his or her rights under Article 12(4), where the controller has not been able to confirm his identity, the requesting person needs to be informed of the negative decision, preferably by the contact information specified in the request.

It is apparent from the investigation that Klarna did not handle the complainant's request because it considered that the complainant's identity could not be ascertained by the information available. The company was then under an obligation under Article 12(4) to inform it because that was the reason why no action was taken in response to the request. It is not clear from the investigation whether the information sent by the company in response to the request to the e-mail address that the company had registered for the applicant contained an indication that the request would not be processed unless identification data were received. However, it is irrelevant for assessing whether Klarna has fulfilled its obligation under Article 12(2) to facilitate the exercise of the data subject's rights. Klarna did not do so because they did not send the request for identification through the contact details provided by the complainant in the request received by fax. As explained above, there are no formal requirements for making a request under Article 17(1). Klarna would therefore at least have sent this information by the contact details provided by the request, so that the person claiming to be registered could be informed of the reason why the request would not be processed unless additional information was submitted, for example if he no longer had access to the e-mail address. It has not emerged from the investigation that it would impose unnecessary personal data processing or unreasonable burden on Klarna to provide the information in this way. The fact that Klarna sent information to the e-mail address that it had registered may be regarded as a security measure, but not sufficient to facilitate the exercise of the complainant's rights in this case.

IMY therefore concludes that Klarna Bank AB has infringed Article 12(2) GDPR by not facilitating the exercise of the complainant's right under Article 17 to have his data deleted in accordance with its request of 9 May because Klarna Bank AB's request for identification data was not sent out via the contact details provided by the complainant at the request.

Choice of intervention

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine.

In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The company infringed Article 12(2) of the GDPR by failing to inform the complainant of the reasons why the complainant's request for deletion was not met. On the other hand, Klarna contacted the complainant without undue delay, even if it was not via the contact details provided by the complainant in its request. Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Klarna Bank AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED], following a presentation by [REDACTED].

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision, no. DI-2022-1722. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2022-1722, IMI case no.
368751,
521.14039 / 631.336

Decision under the General Data Protection Regulation – Klarna Bank AB

Date of decision:
2022-07-25

Decision of the Swedish Authority for Privacy Protection (IMY)

IMY finds that Klarna Bank AB has processed personal data in violation of:

- Article 12(2) GDPR¹ by not facilitating the exercise of the complainant's right under Article 15 for access to their personal data in accordance with their request of 8 February 2021, by misinterpreting the complainant's request for access and requesting a clarification from the complainant without valid reason;
- Articles 12(3) and 17 of the GDPR by not responding without undue delay to the complainant's requests for erasure of 2 May 2019 only on 31 January 2020 and 16 January 2021 only on 31 August 2021.

IMY gives Klarna Bank AB a reprimand pursuant to Article 58(2)(b) of the GDPR for breach of Articles 12(2), 12(3) and 17 of the GDPR.

Report on the supervisory case

The case handling

IMY has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, in its capacity as lead supervisory authority under Article 56 of the GDPR. The handover has been made by the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the GDPR's provisions on cooperation concerning cross-border processing.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

The investigation in the case has been carried out through correspondence. In light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory

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).

authorities concerned has been the data protection authorities in Germany, Denmark, Austria, Italy, Poland and Finland.

The complaint

The complainant mainly states the following.

Several accounts have been registered with Klarna with the complainant's email address or their postal address under someone else's name. The complainant has not personally registered any of those accounts and has requested erasure with Klarna on several occasions, because accounts have recurrently been created in this way for a long period of time. Klarna has not complied with several of the requests and therefore Klarna has not erased all of the complainant's personal data.

The complainant has also requested information on the number of accounts created with their postal address, but has not received such information. It is apparent from an e-mail the complainant sent to Klarna on 8 February 2021, that they requested a detailed list of registered accounts relating to the complainant that Klarna had already erased, and accounts created with the complainant's address data.

What Klarna has stated

Klarna Bank AB mainly states the following.

Klarna is the data controller for the processing to which the complaint relates.

Klarna has received three requests for erasure on 2 May 2019, 30 November 2019 and 16 January 2021. All requests have been handled.

The request for erasure on 2 May 2019 was initiated on 11 December 2019 and was completed on 31 January 2020. At the time of the complainant's request, the complainant claimed that their personal data had been used in connection with fraud and the case was therefore forwarded to the department at Klarna that handles fraud cases. In connection with the closure of the fraud case, the case concerning the complainant's request for erasure was also erroneously closed by the case handler.

The request for erasure on 30 November 2019 was initiated on 11 December 2019 and completed on 31 January 2020. The complainant was informed on 30 November 2019 that the request could take up to 90 days. The reason for this was that the number of incoming cases had periodically been very large and that the handling of data subject request during that time sometimes had taken more than a month. Klarna has handled the request without undue delay, also considering the Christmas and New Year's holidays.

The request for erasure on 16 January 2021 was completed on 31 August 2021. On 16 February 2021, Klarna informed the complainant that the handling could take more than one month. Subsequently, the case handler did not proceed with the process for data subject requests according to Klarna's routines. The complainant's request was therefore not dealt with in accordance with Klarna's procedures at the time due to the individual case handler's error.

Klarna has not interpreted the complainant's request for the number of accounts created with their personal data as a request for access. The question was made to Klarna on 8 February 2021 and the complainant was offered an extract from the register on 16 February 2021, which was not answered by the complainant. The

complainant returned with a reply which Klarna perceived as a request for erasure and further questions on how the complainant's personal data had been used in connection with suspected fraud.

Klarna was contacted by the data protection authority in Berlin on 4 August 2021 where it was informed, inter alia, that that authority interpreted the question from the complainant as a request for access by the complainant. Klarna subsequently responded to the complainant's request for access by sending an extract from the register by mail on 26 August 2021.

Justification of the decision

Applicable provisions

According to Article 12(2) of the GDPR, the controller shall facilitate the exercise of the data subject's rights in accordance with, inter alia, Article 15.

According to Article 12(3) of the GDPR, the data subject's request to exercise his or her rights must be handled without undue delay and in any event no later than one month after the request is received. The period of one month may be extended by a further two months if the request is particularly complex or if the controller receives a high number of requests.

Pursuant to Article 15 of the GDPR, the data subject shall have the right to obtain from the controller confirmation of whether personal data concerning him or her are being processed. If such data are processed, the controller shall provide the complainant with additional information and a copy of the personal data processed by the controller.

In the European Data Protection Board's (EDPB) Guidelines 01/2022 on access, it is considered sufficient for a data subject to indicate that they wish to have access to their personal data in order for a request for access under Article 15 to have been made.² The data subject does not have to explicitly clarify that this is a request for access or refer to the GDPR. If the controller has any doubts as to what right the data subject wishes to exercise, the controller is recommended to contact the data subject and request clarification. If the data subject does not respond, the controller shall interpret the information contained in the first request of the data subject and act accordingly.³ Furthermore, a data subject who has been the victim of identity theft shall be provided with information on all personal data relating to his or her identity,

² EDPB Guidelines 01/2022 on data subject rights — Right of access, adopted for public consultation on 18 January 2022, para. 50, MY translation; original: "In order to make the access request, it is sufficient for the requesting persons to specify that they want to know what personal data concerning them the controller processes. Therefore, he controller cannot refuse to provide the data by referring to the lack of indication of the legal basis of the request, especially to the lack of a specific reference to the right of access or to the GDPR. For example, in order to make a request, it would be sufficient for the requesting persons to indicate that they wish to obtain access to personal data concerning them."

³ EDPB Guidelines 01/2022 on data subject rights — Right of access, adopted for public consultation on 18 January 2022, paragraph 48, IMY translation; original: "If the controller has doubts as to which right the data subject wishes to exercise, it is recommended to ask the data subject making the request to explain the subject matter of the request. Such correspondence with the data subject shall not affect the duty of the controller to act without undue delay. However, in case of doubts, if the controller asks the data subject for further explanation and receives no response, he controller should interpret, bearing in mind the obligation to facilitate the exercise of the person's right of access, he information contained in the first request and act on its basis."

including personal data collected by the controller as a result of the fraudster's conduct.⁴

Pursuant to Article 17(1)(a) of the GDPR, the data subject shall have the right to have his or her personal data erased by the controller without undue delay and the controller shall have the obligation to erase personal data without undue delay if they are no longer necessary in relation to the purposes for which they were collected or otherwise processed. Article 17(3) of the GDPR exhaustively lists the exceptions to this right.

IMY:s assessment

Klarna has not handled two of the complainant's requests for erasure in accordance with the General Data Protection Regulation

A request for erasure shall be handled without undue delay and at the latest within one month from when the request was received the controller pursuant to Article 12(3) GDPR. However, the period of one month may be extended for a further two months under the conditions laid down in the same article.

Klarna states that a request for erasure was received on 30 November 2019 and was completed on 31 January 2020, i.e. two months after it was received. Klarna had previously informed the complainant on 30 November 2019 that the request may take up to 90 days due to the amount of incoming cases and considering Christmas and New Year's holidays. IMY finds no reason to question Klarna's information in this regard. IMY therefore considers that Klarna has given the complainant such a notification that is required by Article 12(3) in the event of an extension of the one-month time limit for handling a request. In light of Klarna's submissions on the large number of requests received during the current period of Christmas and New Year, IMY considers that Klarna has handled the request of 30 November 2019 without undue delay.

Regarding the requests for erasure of 2 May 2019 and 16 January 2021, Klarna did not complete them until more than seven months after the respective requests were made. Consequently, Klarna did not handle the complainant's requests within the statutory time limit. Klarna's argument that the reason for the delays concern oversights by individual case handlers does not alter IMY:s assessment. Therefore, Klarna did not handle the complainant's requests for erasure of 2 May 2019 and 16 January 2021 without undue delay.

Against this background, IMY finds that Klarna Bank AB has processed personal data in breach of Articles 12(3) and 17 of the GDPR by not deleting the complainant's personal data without undue delay, as requested by the complainant on 2 May 2019 only on 31 January 2020, and of 16 January 2021 only on 31 August 2021.

Klarna has not handled the complainant's request for access in accordance with the General Data Protection Regulation

It is apparent from the file that the complainant suspects that they were the victim of identity theft and, as a result, requested a detailed list from Klarna on 8 February 2021

⁴ EDPB Guidelines 01/2022 on data subject rights — Right of access, adopted for public consultation on 18 January 2022, para. 105, IMY:s translation; original: "In case of identity theft, a person fraudulently acts in the name of another person. In this context it is important to recall that the victim should be provided with information on all personal data he controller stored in connection with their identity, including those that have been collected on the basis of the fraudster's actions. In other words, even after the controller learned about the identity theft, personal data is associated with or related to the identity of the victim and hence constitutes personal data of the data subject."

concerning, on the one hand, accounts related to the complainant that Klarna had erased and, on the other hand, accounts created with the complainant's address data.

IMY considers that the complainant's request for a "detailed list" of 8 February 2021 should be interpreted as a request for access under Article 15 of the GDPR. There is no formal requirement for making a request under Article 15. However, Article 12(2) states that the controller shall facilitate the exercise of data subjects' rights under, inter alia, Article 15. Klarna should therefore have understood from the communication that the complainant wanted access to personal data they had a right to under Article 15 of the GDPR.⁵

According to the General Data Protection Regulation, it is Klarna's responsibility as data controller to be able to identify and act on a request for access from a data subject, as is also made apparent from the EDPB guidelines.⁶ IMY considers that there was no reason for Klarna to request clarification from the complainant in the present situation. Moreover, Klarna has described to the complainant only in general terms how they could proceed to request an extract from the register if they intended to make a request for access, in the e-mail sent by Klarna on 16 February 2021. Therefore, the fact that Klarna considered that the complainant had not provided a clear answer after Klarna had offered an extract from the register does not alter IMY:s assessment.

Given these circumstances, IMY notes that Klarna Bank AB has processed personal data in breach of Article 12(2) by not facilitating the exercise of the complainant's right under Article 15 to access their personal data, by misinterpreting the complainant's request for access of 8 February 2021 and seeking clarification from the complainant without reason.

Choice of intervention

Article 58(2) and Article 83(2) of the GDPR gives IMY the authority to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as warnings and prohibitions. Furthermore, it is clear from Article 83(2) which factors are to be taken into account when deciding whether to impose administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may issue a reprimand pursuant to Article 58(2)(b) instead of imposing a fine. Herein considering the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The violations have affected one person and have occurred because of mistakes on the part of Klarna. This applies both to the complainant's requests for erasure and to the request for access. Although Klarna had not complied with the complainant's request for access due to a misinterpretation of the complainant's request, Klarna did not intend to deny the complainant access to their personal data. Against this background, IMY considers that these are minor infringements within the meaning of recital 148 which means that Klarna Bank AB shall be given a reprimand under Article 58(2)(b) of the GDPR for the infringements.

⁵ EDPB Guidelines 01/2022 on data subject rights — Right of access, adopted for public consultation on 18 January 2022, para. 105.

⁶ EDPB Guidelines 01/2022 on data subject rights — Right of access, adopted for public consultation on 18 January 2022, paras. 48 and 50.

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED], following a presentation by legal advisor [REDACTED].

How to appeal

If you wish to appeal IMY:s decision, please write to IMY. Please indicate in your letter the decision you are appealing and the amendment that you are requesting. The appeal must reach IMY no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, IMY forwards it to the Administrative Court in Stockholm for trial.

You can send the appeal by email to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. IMY:s contact details are set out in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) final decision 2022-07-18, no. DI-2021-5301. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-5301, IMI case no.
115747

Date of final decision:
2022-07-18

Date of translation:
2022-07-19

Final decision under the General Data Protection Regulation – Scandinavian Airlines System Denmark-Norway-Sweden

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that Scandinavian Airlines System Denmark -Norway-Sweden has, in relation to complaint 1, processed the complainant's personal data in breach of Article 15 GDPR¹ by not giving the complainant access to their personal data and supplementary information.

The Swedish Authority for Privacy Protection finds that Scandinavian Airlines System Denmark -Norway-Sweden has, in relation to complaint 2, processed the complainant's personal data in breach of Article 12(4) of the GDPR by not informing the complainant, without undue delay, that their personal data are not being processed.

The Swedish Authority for Privacy Protection issues Scandinavian Airlines System Denmark-Norway-Sweden a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 12(4) and 15.

Pursuant to Article 58(2)(c) of the GDPR, IMY orders Scandinavian Airlines System Denmark-Norway-Sweden, in relation to complaint 1, to comply with the complainant's request to exercise their right of access under Article 15, with exception for information which is subject to any applicable derogation provided for in Article 15(4). This is done by providing all personal data that Scandinavian Airlines processes about the complainant by providing the complainant with a copy of the personal data referred to in Article 15(3) and providing information pursuant to point (a) to (h) of Article 15(1) and information pursuant to Article 15(2). The measures shall be implemented no later than two weeks after the decision has become final

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

¹Regulation (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).

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Scandinavian Airlines System Denmark -Norway-Sweden (SAS or the company) due to two complaints. The complaints have been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authorities of the countries where the complainants have lodged their complaints (Norway and Finland) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, Finland, France, Germany, Denmark, The Netherlands, Italy, Spain and Portugal.

The complaints

Complaint 1 (from Norway with national reference number: 18/02229)

The complaint states the following. In connection with a flight from Norway to the United States with SAS on 4 July 2018, the complainant was subjected to extensive security checks both at the airport in Norway and in the United States. The complainant contacted SAS in order to obtain information about what personal data was transferred to the US authorities in order to trigger those extra security checks. The complainant received a reply from SAS on 15 August 2018 that stated that SAS is not responsible for the additional security checks and that they were decided by US authorities. The complainant was not informed about what personal data were transferred and why. In the complaint, the complainant asks for assistance in accessing information about the transfer of their personal data to U.S. authorities as well as the personal data disclosed.

Complaint 2 (from Finland with national reference number: 6134/152/2020)

The complaint states the following. The complainant requested access to their personal data by using the company's contact form. Although 30 days have passed, the complainant has not received any confirmation that the request has been received or any response to the request.

What SAS has stated

SAS has mainly stated the following. SAS is the data controller for the processing to which the complaints relates.

Complaint 1 (from Norway with national reference number: 18/02229)

The company has received e-mail from the complainant but states that it has failed to understand the nature of the case. As a result, the complainant's request was not dealt with as an integrity request due to an oversight. The complainant has not received any information other than that set out in the annexes to the supervisory letter and has therefore not been provided information in accordance with Article 15 of the GDPR.

Since the complainant's case has not been handled as an integrity case, the company has deleted the correspondence with the complainant. The company deletes e-mails

received by customer service after 24 months. The company cannot therefore go back and see the dialogue with the complainant.

Complaint 2 (from Finland with national reference number: 6134/152/2020)

The company received the complainant's request on 5 July 2021 and finalised the case on the same day. The company offers data subjects the possibility to order a copy of their personal data through a form on the company's webpage. After ordering, SAS sends a confirmation to the customer that the order has been received, and as soon as the system has completed the extract, it is sent to the data subject by encrypted e-mail. In case the applicant's personal data are not processed, the applicant receives information about that. In the present case, no e-mail was sent to the complainant stating that their personal data are not in the system. According to the company, a system investigation is ongoing with the aim to clarify why an e-mail was not sent to the complainant and to ensure that the error does not persist. The company intends to inform the complainant when the system error has been investigated.

Justification of the decision

Applicable provisions, etc.

According to Article 5(2) of the GDPR data subjects' personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Article 29 Guidelines on Transparency, adopted by the European Data Protection Board (EDPB), state that when controllers respect the principle of transparency, data subjects can hold controllers and processors accountable and exercise control over their personal data by, for example providing or withdrawing informed consent and actioning their data subject rights.²

According to Article 5(2), the controller must always be able to demonstrate that the personal data are processed in a transparent manner vis-à-vis the data subject. In this context, the principle of liability requires the processing of personal data to be transparent towards the subject, so that controllers can demonstrate that they are complying with their obligations under the GDPR.

To anyone who requests a data controller is obliged to provide information about whether or not their personal data is being processed. If such data is processed, the controller shall, in accordance with Article 15 of the General Data Protection Regulation, provide the data subject with supplementary information and a copy of the personal data processed by the controller.

It follows from Article 15(1) what additional information is to be provided to the data subject. Article 15(1)(c) provides that the data subject shall be informed of the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries.

² Article 29 Working Party Guidelines on transparency under Regulation 2016/679 – WP260, para 4.

According to recital 63, the data subject should have the right of access to personal data processed in order to be aware that processing is taking place and verify the lawfulness of the processing.³

In the EDPB Guidelines 01/2022 on data subjects' rights — Right of access the following is stated:

"...the purpose of the right of access is to make it possible for the data subject to understand how their personal data is being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. In other words, the purpose of the right of access is to provide the individual with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).⁴

"The assessment of the data being processed shall reflect as close as possible the situation when the controller receives the request and the response should cover all data available at that point in time. This means that the controller has to try to find out about all the data processing activities relating to the data subject without undue delay."⁵

The GDPR does not regulate the form in which a request for access is to be made. However, it is generally sufficient for a data subject to express their wish to obtain access to personal data processed or that they wish to have access to information about themselves held by the controller for a request to be regarded as a request for access within the meaning of Article 15.⁶

According to Article 12(3), a request for access must be handled without undue delay and in any event no later than one month after the request has been received. The time limit of one month may be extended by an additional two months if the request is particularly complicated or the number of requests received is high.

If the period of one month is extended, the controller must notify the data subject of the extension. The notification of the extension of the time limit shall take place within one month of receipt of the request. The controller must also specify the reasons for the delay.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy pursuant to Article 12(4) of the GDPR.

Assessment of the Authority for Privacy Protection (IMY)

Has there been a breach of the GDPR?

³ See Judgement of 7 May 2009, Rijkeboer, C-533/07, EU:C:2009:293, paragraph 50-54.

⁴ Guidelines 01/2022 on data subject rights - Right of access, adopted for public consultation 18 January 2022, para 10.

⁵ Guidelines 01/2022 on data subject rights - Right of access, para 37.

⁶ See Guidelines 01/2022 on data subject rights - Right of access, para 50.

Complaint 1 (from Norway with national reference number: 18/02229)

Regarding the first complaint, IMY finds that the complainant has contacted SAS with a request to obtain information on how the company handled its personal data in connection with the trip to the United States. The company has stated that it has failed to understand the complainant's request as a privacy case and thus has not given the complainant access to its personal data and supplementary information in accordance with Article 15 of the GDPR, which IMY finds no reason to question. The company has thus infringed Article 15.

Complaint 2 (from Finland with national reference number: 6134/152/2020)

Regarding the second complaint, IMY finds that the complainant has not been informed that their personal data was not processed by the company in accordance with Article 12(4) of the GDPR. The company has thus infringed Article 12(4).

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider are the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The infringements have affected two data subjects and the data in question was not special category data. The company states that it is carrying out a technical investigation in order to confirm why a confirmation e-mail was not sent and when that is done the company intends to inform the complainant.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Scandinavian Airlines must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

In regard to complaint 1, the company has not handled the complainant's request for access even though the company is obliged to do so. IMY therefore considers that there is reason to order the company to comply, in accordance with Article 58(2)(c), with the complainant's request to exercise its right of access under Article 15. With exception for information which is subject to any applicable derogation provided for in Article 15(4). This is done by providing the complainant access to all personal data that SAS process regarding the complainant by providing a copy to the complainant of the personal data as stipulated in Article 15(3) and provide information pursuant to points (a) to (h) of Article 15(1) and provide information pursuant to Article 15(2). The measures shall be implemented no later than two weeks after this decision has become final.

This decision has been made by the specially appointed decision-maker [REDACTED] after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-08-18, no. IMY-2022-86. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-86, IMI case no.
134934

Date of final decision:
2022-08-18

Date of translation:
2022-08-24

Final decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that the investigation has not shown that Klarna Bank AB has processed the complainant's personal data in breach of Article 32 or 33 of the General Data Protection Regulation (GDPR)¹ in the manner alleged in the complaint.

The case is closed.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Norway) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, The Netherlands, Denmark, Finland, Italy, Spain and Austria.

The complaint

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The complaint states the following. After an online purchase, the complainant chose to use Klarna's invoice options. A few days after the purchase was made, the complainant received several messages and calls from persons who were able to access the complainant's invoice. The complainant contacted Klarna's customer service who was unable to provide any information about the incident. As far as the complainant is aware, unauthorised persons have been able to access the

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).

complainant's invoice by e-mail. The invoice contains the name of the complainant, however, the persons who received e-mails containing the complainant's invoice also had access to the complainant's address and telephone number, because they managed to contact the complainant.

What PUA has stated

Klarna Bank AB has mainly stated the following. Klarna is the data controller for the processing to which the complaint relates.

The company initiated their own investigation after having received calls to its customer service from several persons who incorrectly received the complainant's invoice in February 2019. The investigation found that Klarna did not unlawfully disclose the complainant's personal data. According to the company's investigation it is likely that unauthorised persons have logged in to the complainant's e-mail account and found the invoice from Klarna. The reason for this assumption is that the complainant's login details have been available on a Russian hacker forum. These unauthorised persons have then sent the invoice to other recipients and pretended to be Klarna. However, it is not Klarna who has been the sender of these messages. Since Klarna has not been the sender, it is not possible for Klarna to know exactly how this has been done, but one possibility is so-called e-mail spoofing.²

Klarna has not reported a personal data breach to IMY due to the incident because the disclosure of personal data has not been made from within its own organisation. However, in connection with the incident, Klarna contacted the complainant and provided the requested information and informed about the measures that could be taken to minimise the risk of further unauthorised disclosures of the data.

Justification of the decision

Applicable provisions, etc.

Article 4(1) of the GDPR defines the term 'personal data' as any information relating to an identified or identifiable natural person.

Article 4(2) states that "processing" means any operation or combination of operations concerning personal data or sets of personal data.

According to Article 4(7), the controller is a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Assessment of the Authority for Privacy Protection (IMY)

Klarna has stated that the company is not the data controller for the processing of personal data to which the complaint relates. Furthermore, Klarna states that it did not disclose the complainant's personal data to any unauthorised person and argues that, according to its own investigation, an explanation for the incident may be that someone has accessed the complainant's e-mail account due to the fact that the complainant's login information was available on the internet.

² Email spoofing is the creation of email messages with a forged sender address.

IMY notes that there has been no reason to question what the company has stated. Against this background, IMY finds that the investigation at hand has not shown that Klarna Bank AB failed to comply with the General Data Protection Regulation in the manner alleged in the complaint.

The case is closed.

This decision has been made by the specially appointed decision-maker [REDACTED] after presentation by legal advisor [REDACTED].

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision 2022-10-17, no. DI-2022-4999. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2022-4999 IMI. Case no.
164557, LDA 1085.1-3396/20-F

Date of final decision:
2022-10-17

Date of translation:
2022-10-17

Final decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that the investigation has not shown that Klarna Bank AB has processed the complainant's personal data in breach of Articles 12(3) and 17 of the General Data Protection Regulation (GDPR)¹ in the manner alleged in the complaint.

The case is closed.

Report on the supervisory report

Processing

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (the company or Klarna) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation from the supervisory authority in (Germany) where the complainant has lodged their complaint in accordance with the GDPR's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through written correspondence. Since this is a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned has been the data protection authorities in Denmark, Germany, Poland, Italy, Finland and Austria.

The complaint

In its complaint, the complainant essentially stated the following. Complainants personal data have been confused with data relating to another person who has the same first name and surname. In the role of complainants working life, it is important that his personal data cannot be linked to a due claim. The complainant has requested

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

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).

the deletion of his personal data from Klarna and he has not received confirmation that the deletion has taken place.

What Klarna has stated

Klarna Bank AB has mainly stated the following. Klarna is not the data controller for the current processing to which the complaint relates. Klarna has never processed personal data about the complainant and there has therefore been no personal data to be deleted.

Klarna has previously had a claim for payment against a person with the same first name and surname as the complainant. This requirement has been transferred in 2015 to an external party in accordance with the rules on negotiable debt instrument. The possible confusion has occurred after Klarna has transferred the claim to a third party.
Justification of the decision

Justification of the decision

Applicable provisions, etc.

Pursuant to Article 12(3) GDPR the controller must comply with the data subject's request without undue delay and in any event within one month of receipt of the request.

Pursuant to Article 17 of the GDPR, the data subject shall have the right to have his or her personal data erased without undue delay under certain conditions specified therein.

Assessment of the Swedish Authority for Privacy Protection (IMY)

Klarna Bank AB has stated, on 28 July 2022, that Klarna has never processed the complainant's personal data and is therefore not the data controller for the processing of personal data to which the complaint relates. Furthermore, the company has processed another person's personal data with the same first name and surname in relation to an overdue claim.

IMY notes that there has been no reason to question what the company has stated. Against this background, IMY finds that the investigation at hand has not shown that Klarna Bank AB failed to comply with the General Data Protection Regulation in the manner alleged in the complaint.

The case is closed.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) final decision 2022-10-10, no. DI-2021-3399. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-3399, IMI case no.
115749

Date of final decision:
2022-10-10

Date of translation:
2022-10-11

Final decision under the General Data Protection Regulation – Trionic Sverige AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Trionic Sverige AB has processed personal data in breach of

- Article 6(1) of the General Data Protection Regulation (GDPR)¹ by disclosing the complainant's personal data with a third party without it being necessary to comply with a legal obligation,
- Article 13(1)(e) by providing the complainant with insufficiently specific information about recipients or categories of recipients of the personal data when processing data for the purpose of combating fraud.

The Swedish Authority for Privacy Protection issues Trionic Sverige AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 6(1) and 13(1)(e) of the GDPR.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Trionic Sverige AB (Trionic or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the Regulation's provisions on cooperation in cross-border processing.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Norway and Germany.

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).

The complaint

The complaint states the following.

On behalf of the complainant, a product was ordered via Trionic's German website. According to the complainant Trionic, for some reason became suspicious of the e-mail address used for the order and therefore sent a copy of the order confirmation to the info-e-mail address provided in the domain where the complainant has their e-mail address.

Trionic also sent information about the order to a company even though it was not apparent from the privacy policy that data will be shared with that company. Furthermore, as of 1 July 2018, the privacy policy is not easily accessible. Clicking on the "Privacy Policy" link on Trionic's website opens a new page on the website that links further to the policy located on another website.

Trionic also reportedly Google searched the name, address and contact details of the complainant's representative and possibly linked that information to the complainant's data. Trionic has also stored the entire IPv6 number used when ordering. The privacy policy states that IP numbers are only processed for operation and maintenance purposes. Trionic has also continued to store the IP number even after the complainant canceled the order.

What Trionic Sverige AB has stated

Trionic has mainly stated the following. The company is the data controller for the processing to which the complaint relates.

Transfer to info-e-mail address on the basis of a legal obligation

Trionic sent a copy of the complainant's order to an info-e-mail address on the basis of a legal obligation. Trionic is obliged to take all reasonable steps to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are deleted or rectified without delay (cf. Art. 5(1)(d) GDPR). Trionic's main target group is people in the age range 60-90 years. It is common for the company's customers to make unintentional errors when ordering form in the company's online store.

When the company checked the details of the complainant's order, it reacted to the fact that the e-mail address contained Trionic's company name and the company therefore believed that the buyer had provided an invalid e-mail address. The company then attempted to contact the customer through the given telephone number in order to correct the e-mail address provided. The phone number turned out to be a fax number. In the absence of other contact details, the company visited the domain name of the email address. There the company found the info-e-mail address that the company, for valid reasons, thought was the correct e-mail address. The company then replaced the customer's e-mail address with the one found and sent the order confirmation to that e-mail address. At the time, the company considered that it was its' only possibility to correct the customer's contact details and that the measure therefore was necessary.

When Trionic became aware of the mistake, the company found that it was unlikely that it had resulted in any risk to the complainant's personal integrity. The reason for this was, in particular, that the circumstances indicated that the complainant's personal data had been disclosed to a very limited circle of (other than the complainant) a family member and that it was personal data of relatively limited integrity value.

Legal basis for disclosure to combat fraud

Trionic has disclosed personal data relating to the complainant to a provider of fraud control services on the basis of a legitimate interest which, at the time, acted as a data processor to the company.

The information disclosed consisted of the complainant's name, e-mail address, information that it is the complainant's first purchase from Trionic, the complainant's e-mail domain name, telephone number, order number, number of items purchased, currency of the purchase, the value of the purchase, the complainant's invoice, delivery and IP address.

On the German market, Trionic offers its customers to pay by invoice. It is Trionic that issues the invoice and accounts for the credit risk. Over the years, Trionic has been subject to a number of frauds and fraud attempts in the form of customers who choose to purchase products with invoice payment without the intention to actually pay the invoice. In order to prevent fraud (the purpose of the processing), Trionic has therefore used the services of the provider. The data in question have been disclosed to the service provider on the basis of Trionic's legitimate interest to prevent fraud. Following a balancing test considering the complainant's interests and fundamental rights and freedoms as set out below, Trionic considers that it has had a legal basis for the processing.

The processing was *necessary* to achieve the purpose on the following grounds. The complainant chose to pay by invoice. The data provided by the customer differed from the norm, in that the fax number had been entered instead of a regular telephone number and the e-mail address contained the word "Trionic". Trionic is responsible for the credit risk of invoice purchases on the German market and fraud attempts are common for credit purchases in e-commerce.² About two percent of all purchases in Trionic's online store have been flagged as suspicious by the supplier. Furthermore, Trionic lacks the competence and resources to perform the type of analysis offered by the supplier. Against this background, there were no alternatives to the processing in order to achieve the objective of fraud prevention.

As regards to what the data subject *can reasonably expect*, the company notes that the type of analysis offered by the supplier in the context of credit purchases is common in e-commerce on the European market. The aim is to prevent fraud. It constitutes a type of supplement to credit assessment. A credit assessment can show that a buyer is creditworthy, but not that the buyer is indeed the person to whom the credit assessment relates and that the buyer has a real intention to pay for the purchase. Therefore, in the case of online credit purchases, consumers must expect this type of assessment to be carried out.

Regarding the *nature of the data*, Trionic argues that the supplier's analysis was based entirely on the above-mentioned personal data that Trionic shared with the supplier. This data typically has a relatively limited integrity value, as in many cases it is publicly available.

As regards the *negative consequences*, according to Trionic, the potentially negative consequence of the processing for the complainant is that the credit purchase would be refused, which is a relatively mild consequence that should not affect the outcome of the balancing of interests.

² See for example: <https://www.svenskhandel.se/sakerhetscenter/amnesområden/bedrägerier/>

Legal basis for the processing and storage of IP address prior to cancellation

The complainant's IP address was stored and transferred to the supplier for the purpose of analysing the complainant's geographical location at the time of ordering. These processing operations were carried out for the purposes of fraud prevention (Objective 1) and for the purpose of identifying and asserting legal interests (Objective 2).

The purpose of fraud prevention is a legitimate interest of Trionic. With regard to the necessity of the processing, it can be noted that in the case of fraud attempts, the place of purchase and delivery often does not match the location of the IP address and the customer's connection. Along with other warning signs, such as incorrect phone numbers and a possible IP address connected via anonymisation services, it helps Trionic avoid fraud. Often, fraudulent buyers have several different e-mail addresses but usually do not exchange IP address. Therefore, by saving and processing buyers' IP addresses, Trionic can check the total amount of orders made in the web shop with the same IP address. Without saving the IP address, none of this would have been possible.

With regard to what the data subject *reasonably can expect*, reference is made to the corresponding assessment regarding the disclosure of anti-fraud data as set out above.

As for the *purpose of establishing and exercising legal claims*, Trionic has a legitimate interest in storing the IP address used in purchases in order to establish and enforce legal claims, both civil (debt collection) and criminal law (as a plaintiff in fraud investigations). As regards the necessity of processing, in the case of online credit purchases without the use of e-identification, there is no better opportunity to establish the actual identity of the buyer than to document the IP address used in the purchase. Proof of the identity of the buyer is directly necessary in order to recover past due claims and to obtain conviction in the event of fraud.

Regarding what *the data subject can reasonably expect*, Trionic has made the assessment that from the point of view of the data subject it should appear more or less obvious that e-commerce companies save the IP address of the credit purchaser in connection with purchases in order to be able, if necessary, to establish the identity of the buyer and to recover past due claims and to be able to pursue criminal claims in the event of fraud. Furthermore, Trionic has considered that the IP address has a limited privacy value that does not outweigh Trionic's need to establish and enforce legal claims and that the processing does not risk to cause any significant consequences for buyers. The most obvious consequence may be that the purchase will be denied.

Legal basis for continued storage of IP address after cancellation

Trionic continued to save the complainant's IP address for the purchase after the order was cancelled. However, Trionic deleted it after receiving the complaint, which it interpreted as a request for deletion.

Trionic considers that the company has a legitimate interest in saving the IP address used for the purchase in order to establish and enforce legal claims, both civil (receivable recovery) and criminal law (as plaintiff in fraud investigations). This also applies in the case of cancellations as it may have civil and criminal implications within the limitation period.

The processing is necessary in the same way as before cancellation.

Concerning what the data subject could reasonably expect, it is the same as for storage prior to cancellation, with the addition that, in Trionic's view, the assessment is not affected by the fact that it concerns a cancelled purchase, since it may have civil and criminal implications within the limitation period. However, as mentioned above, after receiving the complaint, Trionic decided to delete the complainant's IP address.

Easily accessible information to the data subject

Trionic states that before confirming the purchase, the complainant had the opportunity to read Trionic's Privacy Policy by clicking on a link in the text "[I] have read the Terms and Conditions and Privacy Policy and approves them." It was then also possible for the complainant to access the Privacy Policy by clicking on a link on the company's website. Due to a loading error, at the time of the complaint, two clicks were required to reach the privacy policy, which has since been corrected. The policy could also be accessed by just one click on a link to the policy at the bottom of the footer of the Trionic website.

Information on the processing to combat fraud and the storage of IP addresses

As regards information on anti-fraud, the processing activities section states:

"Data processing is carried out using computers or IT-based systems in accordance with organisational procedures, which are specifically aimed at the stated purposes. In addition to the responsible person, other internal personnel (personnel management, sales, marketing, legal department, system administrators), or external resource — with the responsible person as principal (such as technical service providers, delivery companies, hosting providers, IT companies or communication agencies) — may operate this website and thus have access to the information. An up-to-date list of these participants may be requested at any time from the provider (Trionic)."³

Trionic is aware of its obligation under Article 13 of the GDPR to inform about the recipients or categories of recipients who are to access the personal data. The text above states, *inter alia*, that Trionic may pass on personal data to external resources. With the complainant's complaint, the company has reviewed the privacy policy and decided to amend it to explicitly indicate that personal data may be disclosed to companies that analyse the fraud risk of credit purchases.

With regard to information about the *storage of the IP address*, the Privacy Policy specifies which data is processed by Trionic or by third parties. It states that so-called "user data" is stored when it is provided voluntarily by the user or collected automatically when using the online store and includes the user's IP address. Furthermore, it is clear that collected personal data may be processed in order to safeguard Trionic's rights and interests. Trionic informed about this in the same way as in the case of anti-fraud.

³ Unofficial translation made by the Swedish Authority for Privacy Protection. Original wording: *Databehandlingen utförs med hjälp av datorer eller IT-baserade system enligt organiseratoriska förfaranden, som är specifikt inriktade på de angivna syftena. Förutom den ansvariga personen kan annan intern personal (personalhantering, försäljning, marknadsföring, juridisk avdelning, systemadministratörer), eller extern resurs - med den ansvariga person som uppdragsgivare (såsom leverantörer av tekniska tjänster, leveransföretag, värdleverantörer, IT-företag eller kommunikationsbyråer) - driva denna webbplats och därmed ha tillgång till informationen. En aktuell lista över dessa deltagare kan när som helst begäras från leverantören (Trionic).*

Search for the applicant's data via search engines

Trionic has not sought the stated contact details on Google and brought them together with the complainant's data as alleged in the complaint.

Justification of the decision

Applicable provisions, etc.

Article 6(1) of the GDPR contains a list of possible legal bases for processing of personal data. One of the legal bases set out in this paragraph must be applicable in order for the processing to be lawful. The points applicable in the case are points 6(1)(c) and (f).

According to Article 6(1)(c), processing is lawful if it is necessary for the performance of a legal obligation incumbent the controller.

In order for processing to be based on Article 6(1)(f), all three conditions provided therein must be fulfilled, namely, firstly, that the controller or third party has a legitimate interest (*legitimate interest*), secondly that the processing is necessary for purposes of legitimate interest (*necessary*) and third that the interests or fundamental rights and freedoms of the data subject do not weigh heavier and require the protection of personal data (*balance of interest*).

Recital 47 of the GDPR states that processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. Furthermore, the Article 29 Working Party⁴ has previously stated that preventing abuse is a legitimate interest under the corresponding rules of the previously applicable Data Protection Directive, as long as the interest is "acceptable under the law" in the broadest sense of the term.⁵

Article 13 sets out the information to be provided by the controller to the data subject where the personal data are collected from the data subject. Under Article 13(1)(e) the controller shall provide the data subject with information on the recipients or categories of recipients of the personal data. According to Article 4(9), the term "recipient" means for an example a natural or legal person to whom the personal data are disclosed, whether a third party or not.

Assessment of the Authority for Privacy Protection (IMY)

Legal basis

Transfer to the info e-mail address on the basis of a legal obligation

Trionic stats that the sending of the complainant's order confirmation to the info-e-mail address — which was a different e-mail address from the one that the complainant filled in — was made on the basis of a legal obligation. The obligation is to comply with the obligation under Article 5(1)(d) GDPR to take all reasonable steps to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are deleted or rectified without delay.

⁴ The Working Party was established under Article 29 of Directive 95/46/EC and was an independent EU advisory body on data protection and privacy issues. With the entry into force of the GDPR, the Working Party has been replaced by the European Data Protection Board (EDPB) (see Articles 68 and 94(2) of the GDPR).

⁵ Article 29 Working Party Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC of 9 April 2014, WP 217, p. 25.

IMY notes that although Article 5(1)(d) constitutes a legal obligation for Trionic, it only permits the processing of personal data that is necessary. IMY observes that there were less coercive measures which the company could have taken that would have led to a lower risk of unauthorised disclosure of the complainant's data. For example, Trionic could have sent the order to the stated e-mail address and consider further measures, for example, if the company received an automatic e-mail server response that the message could not be delivered. The company could also have, for example, refrained from processing the order until the complainant contacted them again, send a regular letter to the address filled in by the complainant or send a fax to the fax number indicated. IMY therefore concludes that the processing was not necessary and that the company did not demonstrate that the processing could be based on this legal basis.

Since it has not been established that Trionic had any other legal basis for the processing, the company has therefor processed the complainant's personal data in breach of Article 6(1) and thus not met the requirement to have a legal basis for the processing.

Legal basis for disclosure to combat fraud

The investigation shows that Trionic has disclosed the complainant's personal data to a provider offering anti-fraud services. Trionic argues that the processing had a legal basis in the company's legitimate interest in preventing fraud, i.e. Article 6(1)(f) of the GDPR.

IMY notes that it is therefore necessary for the company to be able to demonstrate that three conditions are met:

- there are one or more *legitimate interests*
- the processing of personal data is *necessary* for a purpose relating to the legitimate interests
- the interests or fundamental rights and freedoms of data subjects *do not outweigh* the company's legitimate interests (balance of interests).

IMY notes that what may be a *legitimate interest* should be interpreted broadly. The decisive factor is whether the interest is permitted by law or otherwise generally recognised in the rule of law. Insignificant interests do not weigh as heavily as important or compelling interests, but are important only in the balancing of interests. However, if an interest is not justified and legitimate, the balancing of interests shall not be carried out, as the initial threshold of this legal basis will not be reached.

It must also be an *actual interest* at the time of the processing and not an interest which is hypothetical at that time. If there are evidence that the interest is not hypothetical, the condition is satisfied, but it may also be sufficient that the interest typically appears to be factual.

IMY finds that the interest presented by Trionic — to prevent fraud — was justified (cf. recital 47 of the GDPR) and actual at the time of processing.

IMY notes that the requirement of *necessity* means that the interests which the processing is intended to protect could not reasonably be protected in an equally effective manner by other means less intrusive on the fundamental rights and freedoms of data subjects. The condition must be examined together with the principle

of data minimisation which means, among other things, that personal data should not be processed unnecessarily.

According to IMY, the processing — the disclosure of the data to the anti-fraud service provider — was necessary in order to fulfil the purpose which Trionic could not reasonably fulfil in an equally effective manner by, for example, carrying out such an assessment itself. This assessment also considers the fact that the disclosure was not too extensive or privacy sensitive in itself.

IMY notes that the third condition under Article 6(1)(f), *balancing of interests*, is carried out by making an overall assessment, considering in particular:

- the seriousness of the violation that the processing entails for the data subject
- what data subjects reasonably can expect in that situation and
- what security measures have been taken.

When balancing the company's legitimate interests on one hand against the complainant's interests, rights and freedoms on the other, IMY finds that the company's interests weighs heavily especially considering it is a credit purchase. This must be weighed against the complainant's interest in not having their data processed or not risking being denied the purchase of the credit.

The processing appears, in IMY's view, to be something that the complainant could reasonably expect when making a credit purchase on invoice, despite the minor deficiencies in the information identified below by IMY in relation to the information provided on that category of recipients of the data. With regard to the seriousness of the violation, IMY finds that the processing does not appear to be highly violating of privacy and that the data itself is not privacy sensitive. When it comes to protective measures, there has been no evidence of relevance for the assessment in this case.

In an overall assessment IMY finds that the company has shown that the complainant's interests or fundamental rights and freedoms do not outweigh the company's legitimate interests for the processing.

In conclusion, the company has demonstrated that the conditions laid down in Article 6(1)(f) are met and the company therefore had a legal basis for the processing.

Legal basis for the processing and storage of IP address prior to cancellation
Trionic states that it processed and stored the complainant's IP address prior to cancellation on the basis of the legitimate interests of (1) preventing fraud and (2) being able to establish and enforce legal interests.

IMY has already considered that the disclosure of, inter alia, the complainant's IP number in order to prevent fraud had a legal basis. There has been no reason to make any other assessment regarding Trionic's own continued processing and storage of that information before the complainant cancelled their order.

Furthermore, IMY considers that there were no grounds for calling into question the legality of Trionic's processing before the cancellation was made in order for Trionic to be able to establish and enforce legal claims.

The processing of the complainant's IP number therefore had a legal basis.

Legal basis for processing and storing IP address after cancellation

Trionic states that the complainant's IP address was also saved for a certain period after the order was cancelled, on the basis of its legitimate interest of being able to establish and enforce legal claims. However, the data was deleted after the complainant's request.

In view of the fact that Trionic deleted the data in response to the complainant's request and thereby satisfied the complainant's rights, IMY considers that the subject matter of the complaint has been examined to the extent appropriate. IMY does not therefore investigate whether Trionic had a legal basis for storing the complainant's IP number after the cancellation or whether the company's general storage periods are well balanced.

Easily accessible information to the data subject

It is apparent from the company's own information that, at the time of the complaint, two clicks were required for the complainant (considering the links the complainant chose to follow) to be able to access Trionic's privacy policy on its website. The investigation also shows that the information was accessible on the website with fewer clicks (one) in two other ways.

Against this background, and the fact that Trionic also has taken steps to ensure that the policy requires only one click, IMY considers that the subject matter of the complaint in this part has been investigated to the extent appropriate.

Information to the data subject on the processing for the purposes of combating fraud and storage of IP address

The investigation shows that Trionic has disclosed the complainant's data to a supplier for the purpose of combating fraud. In order to comply with the obligation to provide information to the complainant, Trionic had indicated in its privacy policy at the time that personal data could be passed on to 'external resources'. Trionic has now changed this information so that it is explicitly stated that personal data may be disclosed to companies that analyse the fraud risk of credit purchases.

IMY considers that the information provided to the complainant — "external resources" — was not sufficiently specific to meet the requirement of Article 13(1)(e) GDPR to inform the data subject about the recipient (the actual provider) or the categories of recipients (anti-fraud service providers) who would receive the personal data in the case. Trionic therefore infringed Article 13(1)(e).

Searching for the complainant's data on search engines

The complainant has stated that Trionic has searched contact details on a search engine and gathered them together with the complainant's data. The statement was rejected as by Trionic.

IMY considers that there has been no reason to question the company's statement. The investigation in the case does not therefore show that Trionic has processed the complainant's personal data in breach of the General Data Protection Regulation in this part.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with Article 83. Depending on the

circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider are the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The violations have affected one person, the personal data in question was not privacy-sensitive and the company has not previously been found to have infringed the GDPR. Furthermore, Trionic Sverige AB has improved its information to data subjects and acted in response to the complaint.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Trionic Sverige AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been made by the specially appointed decision-maker [REDACTED] after presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2022-11-15, no. IMY-2022-636. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-636,
IMI case no. 134681

Date of decision:
15 November 2022

Date of translation:
2022-11-15

Decision under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that Klarna Bank AB has processed personal data in breach of Article 12(3) and 17 of the General Data Protection Regulation¹ by not having accommodated the complainant's request for erasure made on 25 June 2020 without undue delay. The complainant's request was not accommodated until 31 December 2020.

The Swedish Authority for Privacy Protection issues a reprimand to Klarna Bank AB pursuant to Article 58(2)(b) of the General Data Protection Regulation for the infringement of Article 12(3) and 17 of the General Data Protection Regulation.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated an inspection regarding Klarna Bank AB (Klarna or the company) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In the light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Norway, Denmark, Finland and Italy.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

The complaint

The complainant has mainly stated the following. On 25 June 2020, he requested erasure under Article 17 of the GDPR. Klarna replied the same day, stating that the

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).

complainant's data would be erased but that it could take up to 90 days for the request for erasure to be completed. The complainant requested to exercise his right of access to his personal data on 30 September 2020 and thereby discovered that his data had not been deleted. As Klarna had not complied with the request made on 25 June 2020, the complainant again requested the erasure of his personal data.

What Klarna has stated

Klarna has mainly stated the following.

Klarna is the data controller concerning the processing to which the complaint relates.

Klarna received three requests for erasure, namely on 25 June 2020, on 13 October 2020 and on 20 October 2020. All requests were dealt with.

Erasure of the personal data was initiated on 25 June 2020 following the request for erasure made on that day. A part of the complainant's personal data was erased. Due to a temporary technical error, the complete erasure was not completed immediately but only on 31 December 2020 in connection with the request received on 13 October 2020. The complainant was informed on 25 June 2020 that the processing of the request could take up to 90 days and that the process of erasure had started. The reason for the delay was a high workload.

The request for erasure dated 13 October 2020 was finalized on 31 December 2020. The complainant was informed on 14 October 2020 that the erasure of his personal data had started. Klarna informed the complainant already on 25 June 2020 that the process of erasure could take up to 90 days. This is the reason why Klarna on 14 October 2020 only informed the complainant that the process of erasure had been started and not how long it would take to handle the request.

The request for erasure dated 20 October 2020 was handled together with the request dated 13 October 2020 and was thus also finalized on 31 December 2020.

Klarna has handled the complainant's request received on 13 October 2020 as well as the one received on 20 October 2020 without undue delay, considering the large amount of cases Klarna had to deal with at the time of the complainant's request.

Klarna further states that the company continuously improves its processes to ensure data subjects' rights under the GDPR. Klarna's customer service has improved its structure and prioritization in order to reduce the processing time of the cases received that relate to data protection. The improvements implemented since the complainant's requests were received ensure that the processing time is now considerably shorter.

Statement of reasons for the decision

Applicable provisions, etc.

According to Article 12(3) of the GDPR, the individual's request to exercise his or her rights must be dealt with without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months if the request is particularly complex or the number of requests received is high. The controller shall inform the data subject of such an extension within one month of receipt of the request and shall state the reasons for the delay.

Pursuant to Article 17(1), the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay. Furthermore, the controller shall have the obligation to erase personal data without undue delay where one of the conditions set out in that Article exists, for example where the data is no longer necessary for the purposes for which it was collected or if the consent for processing is withdrawn. Article 17(3) lists the exceptions applicable to this right.

Assessment by IMY

The investigation has shown that the complainant's request for erasure was received by Klarna on 25 June 2020 and that Klarna on the same day informed the complainant that it would take up to 90 days to complete the deletion. According to IMY's understanding, the complainant sent Klarna reminders on 13 and 20 October 2020 regarding its request of 25 June 2020. These reminders do therefore not constitute new requests for erasure. According to Klarna, the request was fully accommodated on 31 December 2020. IMY sees no reason to question this.

Klarna accommodated the complainant's request for erasure only later than six months after the receipt of the request. IMY therefore concludes that Klarna did not handle the complainant's request without undue delay within the meaning of Article 12(3) and 17 of the GDPR. Klarna's argument that a temporary technical error led to the fact that erasure was not completed in time, that Klarna's processes have improved and that the processing time is now shorter does not change IMY's assessment.

Choice of corrective measure

According to Article 58(2)(i) and Article 83(2) of the GDPR, IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be considered when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant circumstances. The violations of the GDPR have affected one person and are the result of mistakes on the part of Klarna. Although Klarna did not accommodate the complainant's request for erasure without undue delay, it does not appear that Klarna intended to deny the complainant the right to erasure. In the light of the foregoing, IMY considers, in an overall assessment, that there is such a minor infringement within the meaning of recital 148. Klarna should therefore be given a reprimand under Article 58(2)(b) of the GDPR for the breach found.

Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that Klarna must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been approved by the specially appointed decision-maker, legal advisor [REDACTED] following a presentation by legal advisor [REDACTED]
[REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Swedish Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Swedish Authority for Privacy Protection if it does not contain any sensitive personal data or information that may be subject to confidentiality. The authority's contact information is shown on the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision, no. DI-2021-4355. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-4355

Date of decision:
2023-01-19

Date of translation:
2023-01-19

Decision pursuant to Article 60 under the General Data Protection Regulation – If Skadeförsäkring AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection ("IMY") concludes that If Skadeförsäkring AB, as per 6 November 2020, has processed personal data in violation of Article 32(1) of the GDPR¹ by sending sensitive personal data to the complainant in an e-mail without using a sufficiently secure encryption solution. Hence, If Skadeförsäkring AB has not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing.

IMY gives If Skadeförsäkring a reprimand pursuant to Article 58(2)(b) of the GDPR for the concluded violation.

Presentation on the supervisory case

IMY has initiated supervision regarding If Skadeförsäkring AB ("If" or "the company") due to a complaint.

The complainant has stated that personal data regarding health has been sent via e-mail without encryption all the way from the sender to the receiver, i.e. by the use of so-called end-to-end encryption. Due to the complaint, IMY has initiated an investigation for the purpose of assessing whether If has ensured an appropriate level of security in accordance with Article 32 of the GDPR as regards the relevant processing.

The investigation in this case has been carried out through written correspondence. Since the complaint concerns cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Finland, Norway and Estonia.

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).

What If have stated

If has mainly stated the following.

Transfer of sensitive personal data via e-mail as per 6 November 2020

If has stated that the company is the data controller for the processing of personal data to which the complaint relates. Furthermore, If has stated that, in the context of its claims settlement, the company sent an e-mail to the complainant in one of the complainant's reported personal injury. The e-mail was sent on 6 November 2020 to the e-mail address provided by the complainant. It contained If's decision and an attached file containing the medical assessment which the decision was based upon. The medical assessment included information regarding background, course of events, diagnosis, assessment, graduation of possible invalidity and date of birth (not the social security number).

The e-mail was sent encrypted with so-called Enforced Transport Layer Encryption (Enforced TLS-encryption). This implied that the message was encrypted from If's servers to the recipient's e-mail server, which in the present case was hosted by Tele2 (the operator). In the event that a receiving server was unable to receive a TLS encrypted message, the message was not sent. Thus, it was ensured that the message was always encrypted during transmission. The company's guidelines in force at the time stated that when sensitive personal data were sent by e-mail, the e-mail should always be encrypted.

The solution with enforced TLS encryption was implemented following a decision² from the Danish data protection authority, Datatilsynet, where If received criticism for using opportunistic TLS encryption for e-mails containing sensitive personal data.

If also refers to a decision³ of Datatilsynet in which the Danish data protection authority concluded, following an investigation of a law firm, that the use of enforced TLS 1.2 entails an encryption with sufficient security for e-mails containing confidential and sensitive personal information during transmission. If stated that it was this encryption solution that was used when the e-mail containing the medical assessment was sent to the complainant on 6 November 2020.

New solution for managing e-mail messages

If has stated that, during the period following the complaint, the company has increased its security by, among other things, developing and launching a new communication solution for e-mails that are sent to the company's customers. Within the framework of this solution, If's customers get access to e-mails via "My Pages" on the company's website. The solution works in such a way that a notification is sent to the customer by e-mail or text message informing the customer that the customer has received a message from If that can be read on "My pages". In order to log in to "My pages", the customer needs to authenticate with the Swedish e-identification "BankID".

² See Datatilsynet's (Denmark) decision of 18 June 2020 in case J.nr. 2019-31-2175.

³ See Datatilsynet's (Denmark) decision of 5 November 2019 in case J.nr. 2019-41-0026.

Justification of the decision

Applicable provisions

Data concerning health constitutes so-called sensitive personal data. It is prohibited to process such special categories of personal data pursuant to Article 9(1) of the GDPR, unless any of the exceptions set out under Article 9(2) is applicable to the processing. These data are considered to be worthy of extra protection as the processing of such data may pose significant risks to the fundamental rights and freedom of individuals.

Furthermore, pursuant to Article 32(1) of the GDPR, the controller shall take appropriate technical and organisational measures to ensure an appropriate level of security for the protection of the data being processed. When assessing the appropriate technical and organisational measures, the controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing and the risks to the rights and freedoms of natural persons.

According to Article 32(1), appropriate safeguards include, among other things:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Pursuant to Article 32(2) of the GDPR, when assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

IMY's assessment

E-mail sent to the complainant on 6 November 2020

Since the controller is responsible for the security of the processing pursuant to Article 32 of the GDPR, the controller needs to assess the risks associated with the processing of personal data and take appropriate technical and organisational measures to address the identified risks. What constitute appropriate measures should not be understood as an arbitrary estimation, but an adequate assessment, based on the nature, scope, context and purpose of the processing and the risks to the individual's rights and freedoms. In this case, the issue is the transfer of sensitive personal data over an open network (internet). The processing of sensitive personal data entails that the technical and organisational measures to be taken by the controller are subject to enhanced requirements.

When an e-mail is sent over an open network, the sender or recipient generally has no control over which computers (e.g. servers) the specific e-mail passes along the way. A consequence of this is that anyone who possesses equipment that unprotected e-mails pass through, can access, disseminate or distort them.

By taking appropriate technical and organisational measures, it should not be possible for unauthorised persons to read personal data transmitted over an open network. This can be achieved by encrypting the e-mail containing personal data and/or by protecting the transmission of the e-mail through encryption. Enforced TLS is an example of an encryption solution that can be used to protect an e-mail. In the present case, enforced TLS was used when the relevant e-mail was sent.

IMY notes that the solution used by If to send the e-mail to the complainant only encrypted the e-mail during the transport from If's e-mail server to the e-mail server provided by the complainant's operator. This implied that the encryption ended before the message had reached the final recipient and, thus, did not constitute an end-to-end encryption. Consequently, there was a risk that unauthorised persons could access the e-mail in plain text after the encrypted transmission had ended.

In light of the above, it cannot be deemed that If had protected the data in such a manner that only the intended recipient could access it after the e-mail had been delivered to the operator's e-mail server. At that moment, the encryption ceased and therefore the data lacked sufficient protection against unauthorised disclosure of, or unauthorised access to, the personal data. Since the e-mail contained sensitive personal data, there was a significant risk of breach of the complainant's privacy.

If refers to a decision issued by the Danish data protection authority, Datatilsynet, which concerns a law firm, to demonstrate that Datatilsynet has deemed enforced TLS to be a sufficiently secure solution for transfer of sensitive personal data. IMY notes that the relevant decision does not concern a specific processing, but rather a planned investigation of the security of the processing of personal data, in particular when using encrypted e-mails. The law firm has specified various methods that it uses to ensure secure communication. The method to be applied is assessed in each individual case and one of the methods is to encrypt the transmission of e-mails using enforced TLS. Datatilsynet has assessed that the law firm's action was in accordance with the GDPR. IMY's investigation in this particular case differs from the Danish decision since this investigation concerns the question whether a specific consignment has been adequately protected all the way from the sender to the receiver.

In conclusion, IMY considers that, during the specific occasion, If had not taken appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by the processing, since If had sent the e-mail containing sensitive personal data without ensuring that the deployed encryption solution protected the message all the way to the recipient. Consequently, If processed personal data in breach of Article 32(1) of the GDPR.

If's new solution for managing e-mails

If has stated that, during the period following the complaint, the company has, among other things, developed and launched a new communication solution for e-mails to its customers. It is noted that the personal data processing carried out within the scope of this new solution is not subject of the complaint and is therefore not part of IMY's investigation.

Choice of intervention

Article 58(2) and Article 83(2) of the GDPR give IMY the authority to impose an administrative fine. Depending on the circumstances of the case, an administrative fine shall be imposed in addition to or in place of the other measures referred to under Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be taken into account when deciding on an administrative fine and determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand under Article 58(2)(b). The aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous infringements of relevance, shall be considered.

IMY has found that If has processed personal data in breach of Article 32(1) of the GDPR. An infringement of that provision may give rise to a fine. If's infringement was committed when the company sent an e-mail containing sensitive personal data to the complainant on 6 November 2020 without using a sufficiently secure encryption solution that protected the message all the way from the sender to the intended recipient (so-called end-to-end encryption).

IMY's investigation concerns an e-mail sent by If without the use of adequate security measures — the one to which the complaint relates. If has worked to improve the security by, following Datatilsynet's decision against If, changing from opportunistic to enforced TLS and also, following the complainant's allegations of security flaws, taking security measures by, among other things, developing and launching a new communication solution for e-mails to the company's customers. Overall, IMY therefore considers the infringement to be minor why, on the basis of 58(2)(b) of the GDPR, If is given a reprimand.

This decision has been approved by unit manager [REDACTED], following a presentation by It and information security specialist [REDACTED].

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review. You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-01-19, no. IMY-2022-1032. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-1032

Date of decision:
2023-01-19

Decision under the General Data Protection Regulation – Lensway Group AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Lensway Group AB when handling the request for erasure made on 20 February 2020 by the complainant in Complaint 1, and the request for erasure made on 25 June 2020 by the complainant in Complaint 2, has processed personal data in breach of:

- Article 12(6) GDPR¹ by requesting a copy of the identity document and signature when this was not necessary to confirm the identities of the complainants; and
- Article 12(2) of the GDPR by requiring that the complainants when requesting erasure submit information by mail in order to confirm their identities, which did not facilitate the exercise of the complainants' right to erasure.

The Swedish Authority for Privacy Protection issues a reprimand to Lensway Group AB pursuant to Article 58(2)(b) of the GDPR for infringement of Articles 12(2) and 12(6) of the GDPR.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Lensway Group AB (the company) due to two complaints, mainly to investigate whether Lensway Group AB has received and handled the complainants' requests for erasure in accordance with Articles 12 and 17 of the GDPR. The complaints have been submitted to IMY as the lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made by the supervisory authority of the country where the complainants have lodged their complaints (Finland and Denmark) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The case has been handled through written procedure. In view of the complaint relating to cross-border processing, IMY has made use of the cooperation and

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).

consistency mechanisms provided for in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Norway and Finland.

The complaints

The complainants have mainly stated the following.

Complaint 1 (Complaint from Finland with national registration number 1576/153/2020)

The complainant was in contact with the company on 20 February 2020 and requested erasure. The company replied to the complainant that the complainant needs to send them the postal address so that they can send the complainant documents relating to the complainant's request. These documents were to be signed and returned by the complainant. In addition, the company requested the complainant to verify the identity by sending a copy of the complainant's identity document by e-mail. For security reasons, the complainant was not willing to provide what was requested.

Complaint 2 (Complaint from Denmark with national registration number 2020-31-3616)

The complainant requested erasure of the complainant's information on lensway.dk. In order to comply with the request, the company requested that the complainant provide the social security number and a copy of the identity document. However, the company could not tell the complainant why they need that information except that they need it in order to confirm the complainant's identity. The complainant questions the need for the company to collect personal data in order to erase personal data. The complainant suggested that the company could instead confirm the complainant's identity by sending an e-mail to the address registered on the complainant but they refused.

What Lensway Group AB has stated

In its statements of 20 April, 12 May and 11 August 2022, the company has mainly stated the following. The Company is the data controller concerning the processing to which the complaints relates.

Complaint 1

The company has received the complaint's request for erasure, but the complainant has not completed the company's at the time current verification process. The company has requested the complainant to submit a copy of the identity document. This is the only way the company has so far been able to ensure the identity of the customer. The copy was to be sent by regular mail. The company also requested the complainant to submit a signed request for erasure. The company has so far not been able to receive this information digitally. In order to ensure that they have received original documents, they have asked the complainant to submit it via regular mail.

Complaint 2

The company received the request for erasure on 25 June 2020 but the complainant did not complete the company's at the time current verification process. It is true that the company requested the complainant's social security number in the written form, but it has been voluntary to provide this information. In addition to the information requested in the written form, the company requested the complainant to submit a

copy of the identity document. The company has so far not been able to identify the complainant in any other way. The complainant was asked to submit the information by regular mail in order to ensure that the company had received the original documents.

As regards both complaints the company has stated the following:

As regards the written form to be submitted by both complainants, the company states the following concerning the personal data required to disclose and why the information was necessary.

- Name is mandatory information which is requested to confirm the identity of the data subject.
- Email address is mandatory information which is requested because it is used as a unique identifier of customers in the company's system.
- Signature is mandatory for the company to be able to ensure that the data subject has read the information and has given his or her consent.

The company states that they should always ensure that it is the right person that contacts them when it comes to requests to exercise a right under the GDPR. Since the company was previously unable to identify the customer in a good and secure way when they contacted the company through customer service, the manual process via regular mail has been the one they have used. In this way, they have had a two-step verification. Functionality to enable confirmation of the customer's identity through customer service has not been in place.

The customer relationship with the company can be established in two ways, either the customer makes a purchase or the customer logs in to My Pages. When the customer creates an account on My Pages, the customer enters their email address and an email with confirmation is sent to the customer. The customer can then, via the link in the email, come to a web page where they link a password to the email address. The customer account is then created and the company thus receives a two-step verification. The complainants used the second method by which the customer relationship can be established.

The complainants made purchases with the company and they were identified through the company's payment service provided by Klarna. For most payment options, Klarna requires the customer to verify themselves via bank ID. For certain payment methods, for example payment by credit card, the customer may choose not to have to verify via bank ID through Klarna's app.

The company's existing digital contact channel is My Pages. However, there has been no functionality to handle requests to exercise a right under the GDPR on My Pages. Since April 2022, the company's customers can now request to be erased or receive a copy of their personal data directly via My Pages. The customer's identity is then verified via regular login.

Statement of reasons for the decision

Applicable provisions, etc.

According to Article 17(1), 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 grounds set out in the Article applies, for example when the personal data are no longer necessary in relation to the purposes for which they were collected or if the data subject withdraws consent on which the processing is based.

Article 12(2) requires the controller to facilitate the exercise of data subject rights under Articles 15 to 22.

Article 12(6) states that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The European Data Protection Board's (EDPB) Guidelines 01/2022 on access² state inter alia:

65. In cases where the controller requests the commission of additional information necessary to confirm the identity of the data subject, the controller shall each time assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (see section 3.3). Such additional information should not be more than the information initially needed for the verification of the data subject's identity (authentication). In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which is not relevant or necessary to strengthen the link between the individual and the personal data requested.

[...]

73. It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate, unless it is strictly necessary, suitable, and in line with national law. In such cases the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that identification by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.

² EDPB, Guidelines 01/2022 on data subject rights — Right of access, Version 1.0. The guidelines have been out for public consultation and are awaiting final adoption.

Assessment of IMY

On the basis of the complaints in question, IMY has examined the company's conduct in these two individual cases.

Has the company acted in accordance with 12(6) of the General Data Protection Regulation when the company requested current information from the complainants?

Has Lensway Group had reasonable grounds to doubt the identity of the complainants?

It is only when the controller has reasonable grounds to doubt the identity of the person making the request that additional information to confirm the identity may be requested. What constitutes "reasonable grounds" in Article 12(6) GDPR should be assessed on the basis of the circumstances in the individual case. The assessment of whether there are reasonable grounds in an individual case to doubt the identity of the one requesting is normally made in the light of the information provided in connection with the request. This applies particularly in situations where the controller has no further knowledge of the person. However, the need for an individual assessment does not preclude the establishment of routines for how the controller normally verifies the identity of the data subject.

The company was given the opportunity to motivate the individual assessment made based on the complainants' situation if they considered that they had reasonable doubts as to the identity of the complainants when the complainants submitted their requests. With regard to both complainants, the company argues mainly as follows. The company should always ensure that it is the right person that contact them when it comes to requests to exercise a right under the GDPR. The customer has not previously been able to be identified in a good and secure manner when they contacted the company through Customer Service. Functionality for handling requests to exercise a right under the GDPR has not been available through Customer Service or on My Pages.

IMY notes that it is not clear from the investigation in the case what information the complainants provided in connection with their request and whether there were reasons for the company to doubt their identity on the basis of those requests. However, IMY considers that, in light of what has emerged in the case, there is no need to question the company's statement that it had reason to doubt the identity of the complainants. In the assessment, IMY takes into consideration the fact that the obligation to ensure the identity of the one requesting also is intended to protect data subjects against someone else making requests in their name, which may lead to negative consequences for the data subject. The risks of these negative consequences in the event of false requests are particularly obvious in the case of more invasive measures, such as the exercise of the right to erasure. IMY therefore takes the view that it has not been shown other than that the company, in the present cases, have had reasonable grounds to doubt the identity of the complainants.

Has the information requested by the Lensway Group been necessary to confirm the identity of the complainants?

Although the controller has reasonable grounds to doubt the identity of the data subjects, the controller shall not collect more personal data than is necessary to enable the confirmation of the identity of the requesting data subject.

The company mainly states the following concerning the necessity of the information they have requested from both complainants. A copy of the identity document has been requested as it was the only way in which the company has so far been able to verify the identity of the customer. In addition to a copy of the identity document, the complainants were required to submit a written form. The information requested in the written form and why it was necessary is presented by the company in essence as follows. The name has been requested to confirm the identity of the data subject. The email address has been requested because it is used as a unique identifier of customers in the company's system. The signature has also been requested and is, according to the company, a necessary information for the company to be able to ensure that the data subject has read the information and given his or her consent to the handling of the request.

As regards the verification of the identity of the complainants, the company states that both complainants made purchases where they were identified through the company's payment service provided by Klarna.

It appears from the company's statements that it was not required that the company itself verified the identity of the complainants when the customer relationship was established, i.e. at the time of purchase. IMY states that the company cannot require more personal data when the complainant wishes to exercise its rights than was required when establishing the customer relationship. A copy of the identity document and signature is information that the company has not requested at the establishment of the customer relationship in these two cases. Furthermore, IMY takes into account that, according to the EDPB Guidelines on the right of access, the use of a copy of an identity document as part of the authentication process should be considered inappropriate, unless strictly necessary, suitable and in line with national law. IMY considers that the requirement to provide the controller with a copy of its identity document is an intrusive measure, which is only appropriate where the controller has previously ensured the actual identity of the data subject and where alternative less intrusive means of verification are inappropriate. IMY considers that there have been no circumstances identified that speak against that other, less intrusive, verification methods could have been used in the present cases, such as login via My Pages or control questions. IMY notes that it has therefore not appeared in the case that the request for a copy of the identity document or the signature would have been absolutely necessary or appropriate.

Against this background, IMY considers that the copy of the identity document and the signature cannot therefore be considered to have been necessary to confirm the identity of the complainants in accordance with Article 12(6) of the GDPR.

Has the company acted in accordance with 12(2) of the General Data Protection Regulation when the company requested the complainants to send the information by mail?

The next question is whether it has been permissible to require the complainants to send the requested information to the company by regular mail.

In view of the requirements to facilitate the exercise of the data subject's rights in Article 12(2) GDPR, it can only be accepted in exceptional cases that a controller as the sole channel of contact refers individuals to ordinary mail if they have to submit information in order to ensure their identities, for example if it is justifiable for reasons of security. The starting point should be that alternative means of submitting requested information should be offered. In that regard, the company has mainly stated that it required the information to be sent by regular mail in order to ensure that they received the original written documentation.

IMY takes the view that the transmission of a copy of an identity document may indeed pose particular risks, which may justify requiring that the document be sent by mail. This provided that it is necessary information to confirm the identity of the data subject.

In the present cases, IMY concludes above that a copy of the identity document was not necessary to confirm the identity of the complainants. By requiring the complainants additionally to send the information by regular mail, IMY takes the view that the company did not facilitate for the complainants to exercise their right to erasure. IMY therefore considers that the company thereby acted in breach of Article 12(2) of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be taken into account when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. It has emerged from the investigation in the case that a copy of an identity document and signature is no longer requested by Lensway Group AB upon requests from data subjects to exercise their right to erasure under the GDPR. Furthermore, the infringements found have occurred relatively far back in time (2020) and have affected two data subjects. Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that Lensway Group AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED], following a presentation by legal advisor [REDACTED]

How to appeal

If you wish to appeal IMY:s decision, please write to IMY. Please indicate in your letter the decision you are appealing and the amendment that you are requesting. The appeal must reach IMY no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, IMY forwards it to the Administrative Court in Stockholm for trial.

You can send the appeal by email to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. IMY:s contact details are set out in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision 2023-05-22, no. IMY-2022-9109. Only the Swedish version of the decision is deemed authentic.

Ref no:
IMY-2022-9109

Date of decision:
2023-05-22

Decision pursuant to Article 60 under the General Data Protection Regulation – MAG Interactive AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that MAG Interactive AB (556804-3524) in handling the request for erasure that the complainant made on 31 January 2021 has processed personal data in violation of:

- article 12.6 of the General Data Protection Regulation (GDPR)¹ by requesting information in the form of usernames of three friends and three opponents in the game QuizDuel when this was not necessary to confirm the complainant's identity and
- article 12.2 of the GDPR by, after the complainant requested erasure by email, also requiring the complainant to log in to the game to send the request from within the game, which has not facilitated the complainant's exercise of the complainant's right to erasure.

The Swedish Authority for Privacy Protection issues a reprimand to MAG Interactive AB pursuant to Article 58(2)(b) of the GDPR for infringement of Articles 12(2) and 12(6) of the GDPR.

Presentation of the supervisory case

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding MAG Interactive AB (the company) due to a complaint, essentially to investigate if MAG Interactive AB has received and handled the complainant's request for erasure correctly, i.e. if the company had reasonable grounds to doubt the identity of the complainant and in such case if the information requested from the complainant was necessary to confirm the identity of the complainant and whether the company has facilitated the exercise of the complainants' rights to a sufficient extent (Articles 11, 12 and 17 of the GDPR). The complaint has been submitted to IMY, as the lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complainant has lodged

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

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).

their complaint (France) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In the light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The concerned supervisory authorities concerned have been the data protection authorities in Denmark, France, Ireland, Norway, Poland, Germany and Austria.

The complaint

In the complaint the following is mainly stated.

On 31 January 2021, the complainant requested erasure of their personal data in the game QuizDuel, a game that the complainant used through their Facebook account. MAG Interactive AB requested further information from the complainant for the purposes of identification even though the complainant in their request for erasure, stated their Facebook ID and email addresses. To the complaint the complainant has attached the correspondence between the complainant and the company of what among other things the following appears. On 28 February 2021, the company replied that it is not in a position to locate, using the complainant's Facebook ID, the complainant's account and that the complainant needs to open any of the MAG Interactive-games to make a request. The complainant replied that they no longer have an MAG Interactive account. On 11 March 2021, the company requested the following information from the complainant in the purpose of restoring the complainant's account and thus enabling the complainant to request erasure of their personal data: username, name of three friends, names of three opponents and an email address to which they want to link the account.

What the company has stated

The company has mainly stated the following in its statements from the 4 and 7 of November 2022.

Description of the course of events relating to the handling of the complainant's request for erasure

On 31 January 2021, the complainant contacted one of the company's support email addresses and provided a Facebook ID and three email addresses and requested to be erased. By this time, given the information the support received, the company did not receive any hits at a direct search in the company's system, neither on the Facebook ID nor on any of the specified email addresses. The company's support responded on 1 February 2021 with instructions for how the complainant can request erasure from the game. The complainant contacted the company again on 8 February 2021 and said they don't have the game left but want to get rid of their data. On 9 February 2021 the company's support replied that the easiest way is to download the game again and request erasure from within the game. On 12 February 2021, the complainant replied and said they wanted to know what information the company had about them. From this time on, the case was handled by the company as a request for access.

On 13 February 2021, the company's support replied that the complainant may request access from within the game. The complainant contacted the company again on 20 February 2021 and had problems with using their Facebook account. The complainant asked again if the company could find their account with their Facebook

ID. On 23 February 2021, the support team replied that they did not find any account with the Facebook ID provided by the complainant but that they should be able to start any of the company's games and request the personal data from within a game.

On 27 February 2021, the complainant asked whether the company had actually tried searching on their Facebook ID. The support responded again on 28 February 2021 that they cannot find their account on the Facebook ID they specified but that they should be able to start any of their games and request access from within the game. On 4 March 2021, the complainant replied that they played 'QuizDuel' on Facebook and does not have an account with MAG Interactive. Therefore, they cannot request access from there. This was probably a misunderstanding as the game never existed on Facebook but they may have logged in via a Facebook button originally which was possible several years ago. It was the first time that the complainant mentioned the game in question, which made it much easier to look for their data.

On 11 March 2021, the support replied that they do not find the complainant's account via their Facebook ID but that they should try to help them access their account so that they can request access or delete their account. The support had then likely managed to locate an account linked to one of the complainant's specified email addresses using the information about the game. The support then sent the standard questions the company asks when the company helps users access their account if they have forgotten their user details. The complainant never replied to that email and when sufficient time had passed, the company closed the case.

On 30 October 2022, after the company's CTO had received the case, the CTO located an account that could be linked to the complainant and emailed the complainant to obtain confirmation that the account should be erased. On 6 November 2022, the complainant replied, confirming that they own the account and that the account should be erased. On 7 November 2022, the complainant's account was erased and the complainant was informed thereof.

Processing of the complainant's personal data by the company at the time of the complainant's request

At the time of the complainant's request for erasure, it processed an email address associated with the complainant and probably advertisingId/vendorId from their telephone, the complainant's username and password. Otherwise, the company did not process any other of the complainant's personal data because any chat history and IP number has long been deleted due to the company's retention policy.

Why the company claims to have had reasonable grounds to doubt the identity of the complainant

In their request for erasure, the complainant indicated a Facebook ID and three email addresses and wrote that they had used one of the company's apps on Facebook.

The company's games are played not on Facebook but on mobile phones and they did not provide any surrounding information such as username, which game it was or even that it was a game. The game that the complainant, according to later reportedly, had played is so old that the company neither got any hits on the other email addresses. Moreover, since the game which the complainant's user account is tied to since long is closed, it makes it difficult to find it only with an email address. Email addresses are public and an indication of an email address is therefore not proof of ownership. The

email address from which the request came was also not linked to any account with the company or to the Facebook ID provided. As regards the other two e-mail addresses, there was no evidence that these were the complainant's email addresses.

The Facebook ID provided by the complainant is not registered with the company. Since many years, Facebook has stopped using global user numbers for privacy reasons. In the service that the company suspended many years ago, where it was possible to log in via a Facebook account, the company does not see the same number as the complainant indicates. The customer number the company received from Facebook is only linked to the company and cannot be linked to a person's Facebook account.

Given the knowledge of which game it concerns that the company eventually got, it would have been possible to find the account to which one email address was linked. The company could then have sent an email to that email address in order to confirm the complainant's identity. However, it had not played any role in this case when on 13 February 2021 the case was changed to a request for access.

How the complainant should proceed to request erasure and subsequent access

The support initially suggested that the complainant should request erasure directly from the game as it is the simplest and safest way. Normally, users still have the game on the phone. In addition, the company's games at a reinstallation help the user get back to the correct account. Therefore, when support has difficulty finding an account with the user's details, it is reasonable that they suggest a reinstallation to get to the correct account. Support can also delete information directly if ownership of the information can be substantiated. In the present case, the case turned to a request for access and then the company normally wants the user to be logged in to its account. The company has stated that just as for the request for erasure, proof of ownership of the account is required to request access, for reasons of privacy and in accordance with the GDPR. As user data may contain chat logs, the handling of the access request is a little more stringent than when handling a request for erasure of user data. The company therefore requires that the request be made from within the player's account.

Information requested for the purpose of verifying the identity

The game that the complainant had played was a game with user accounts. In games with user accounts, there are often chats for players to be able to talk to each other. For privacy reasons, it is important that anyone can not read someone else's chats. The accounts are therefore password protected. Users can enter an email address for password reset, but not all users do, or they have changed their email address.

One question all online services struggle with is how to handle cases where users forgot their login details and it is not possible to reset the account via email. Some use security questions, where users are allowed to fill in the name of their first pet or similar. In the company's case, it is a little more complicated because, as the company does not want to ask users for more information than absolutely necessary and the game concerned in the present case has a user base built since 2012 with 100 million users who have not entered such information. Once the user has forgotten the login details and the account cannot be restored via email, the company resolves this by using information on the phone and the operating system to help users back to the

account, which is why support sometimes asks users to install the game, which also the support has done in this case.

When it doesn't work, or as in this case, when the user doesn't want to, the support ask as a last resort for information that the user should know and that should be easy for a user to remember but that is difficult for others to know about. This information is requested in order for the company to ensure that it is the account holder that they give access to the account. The information requested by support in such cases is the following:

- User name of the data subject. Information that is assumed to be easy for most people to provide. However, it is also information that is relatively easy for others to find out.
- Username of three of the registered friends in the game. Most people who play this game have some friends they've been playing with for years. This information should also be easy to answer.
- Username of three of the registered opponents in the game. This information is often a little harder to provide but for users who mostly play against random players and do not add friends, it is necessary information.

The support also asked for the email address the user wanted to link the account to. This is in order for the complainant to be able to log in and request their user details from within the game.

The data shall normally be provided by email in the ongoing support dialogue. It is not a requirement to be right on all questions, but an assessment is made based on how right/wrong the answer is. Nor does the Company ask for personally identifiable information, but only for usernames that are normally anonymous/pseudonymous and which are already in the company's register. The only information that is personally identifiable information is the email address the user wants to link to the account. If the user can respond so well that the company determines that the user actually owns the account, the support will set the email address for recovery. The user can then set a new password and log in.

The company is continuously working on improving its support tools and will shortly release a new version where this particular scenario can be managed and which will make it easier for support to find users even with very limited information. Support is instructed to erase the user's account immediately if the email address on the account matches the user's email address and otherwise help the user erase the account through the game. In this case, the company can imagine a third solution, that the company email out a link to the linked account and that the user confirms erasure via the link to verify their identity. The company intends to add such possibility.

The complainant's account has been deleted

The complainant's request for erasure has now been met. The company has emailed the complainant on 30 October 2022 both at the email address they used in the support case and the email address they were found when searching. The company's CTO asked the complainant to reply from that email address. A reply from the complainant was received on 6 November 2022 confirming that they own the account.

The CTO subsequently erased the complainant's account and informed the complainant accordingly.

Statement of reasons for the decision

Applicable provisions, etc.

Pursuant to Article 17(1), 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 grounds listed in the Article applies, for example where the data are no longer necessary for the purposes for which they have been collected or where consent for processing is withdrawn.

Article 11(1) states that where the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, 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 this Regulation.

According to Article 11(2), where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

Article 12(6) states that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

Article 12(2) requires the controller to facilitate the exercise of the data subject's rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

The European Data Protection Board's (EDPB) Guidelines 01/2022 on access² state, inter alia, the following:

53. The EDPB encourages controllers to provide the most appropriate and user-friendly communication channels, in line with Art. 12(2) and Art. 25 GDPR, to enable the data subject to make an effective request. Nevertheless, if a data subject makes a request using a communication channel provided by the controller, which is different from the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle such a request accordingly (see the examples below). The controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated (for example, when a data subject sends an access request to an employee who is

² EDPB, Guidelines 01/2022 on data subject rights – Right of access, version 2.0, adopted on 28 March 2023.

on leave, an automatic message informing the data subject about an alternative communication channel for this request could be a reasonable effort).

[...]

67. In cases where the controller requests or is provided by the data subject with additional information necessary to confirm the identity of the data subject, the controller shall, each time, assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (see section 3.3).

68. In order to allow the data subject to provide the additional information required to identify his or her data, the controller should inform the data subject of the nature of the additional information required to allow identification. Such additional information should not be more than the information initially needed for the authentication of the data subject. In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.

[...]

70. As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.

[...]

138. The use of self-service tools should never limit the scope of personal data received. If not possible to give all the information under Art. 15 through the self-service tool, the remaining information needs to be provided in a different manner. The controller may indeed encourage the data subject to use a self-service tool that the controller has set in place for handling access requests. However, it should be noted that the controller must also handle access requests that are not sent through the established channel of communication.

Assessment of IMY

On the basis of the complaint in question, IMY examined the company's conduct in this individual case.

Has the company been able to identify the complainant?

The company states that, on the basis of the information contained in the complainant's request for erasure on 31 January 2021, the company was not in a position to identify the data subject. According to the company's statement, the information provided by the complainant in the request did not result in a direct finding in the company's system, neither on the Facebook ID nor on any of the email addresses provided by the complainant. The company further states that when they on 4 March 2021 received information on which game the complainant's request concerned, they were able to find an account to which one of the complainant's e-mail addresses was linked to. In light of this, IMY notes that, at least on 4 March 2021, the company was able to link the complainant's request to a user account and that identification of the complainant was thus possible. IMY therefore considers that, in accordance with the provisions of Article 11(2) of the GDPR, the complainant provided such additional information which made identification possible. The company has thus not demonstrated that it was not in a position to identify the data subject and could therefore not refuse to comply with the data subject's request to exercise their rights under Article 12(2) of the GDPR.

Has the company acted in accordance with 12(6) of the GDPR when the company requested current information from the complainant?

Has the company had reasonable grounds to doubt the identity of the complainant

It is only where the controller has reasonable grounds to doubt the identity of the person making the request that additional information to confirm the identity may be requested. What constitutes "reasonable grounds" in Article 12(6) GDPR should be assessed on the basis of the circumstances of the individual case. The assessment of whether there are reasonable grounds to doubt the identity of the one making a request is normally made in the light of the information provided in connection with the request. This applies particularly in situations where the controller has no further knowledge of that person. However, the need for an individual assessment does not preclude the establishment of procedures for how the controller normally verify the identity of the data subject.

It appears from the annex to the complaint that the complainant provided the following information when requesting erasure on 31 January 2021: Facebook ID and three email addresses as well as one email address from which the request email was sent.

The company states that, at the time of the complainant's request for erasure, they processed an email address associated with the complainant and probably also the advertisingId/vendorId from the complainant's telephone, the complainant's username and password.

The company was given the opportunity to motivate the individual assessment made from the complainant's situation if the company considered that it had reasonable grounds to doubt the identity of the complainant when they made their request. The company stated mainly the following. The company's games are not played on Facebook but on mobile phones, so Facebook ID did not contribute to the verification of the complainant's identity. Email addresses are public and a statement of such is not a proof of ownership. The email address from which the request was made was also not linked to any account with the company or to the Facebook ID provided. The complainant did not provide any surrounding information such as user name, which game it concerns or even that it is a game. The game played by the complainant, according to later provided information, was so old that the company did not receive

any search findings on the other email addresses provided in the request. On 4 March 2021, on the basis of the information provided by the complainant on which game the request concerns, the company found a user account linked to one of the complainant's e-mail addresses.

In the light of the company's submissions and the information provided by the complainant in their request for erasure, IMY finds that the company had reasonable grounds to have doubts concerning the identity of the complainant. In the assessment, IMY also takes into account the fact that the obligation to ensure the identity of the person making the request is also intended to protect data subjects against someone else making inaccurate requests in their name, which may lead to negative consequences for the data subjects.

Has the information requested by the complainant been necessary to confirm their identity?

Although the controller has reasonable grounds to doubt the identity of the data subject, the controller shall not collect more personal data than is necessary to enable the identification of the requesting data subject. The controller shall carry out a proportionality assessment and be able to justify the verification method used.

The company has stated that the request was changed to a request for access on 4 March 2021, and the company then required that the request be made from within the user's account. As user data may contain chat logs, the handling of the access request is a little more stringent than when handling a request for erasure of user data, the company has stated. As regards the necessity of the information the company has requested from the complainant in order to confirm their identity, the company has stated, mainly the following. Usernames are requested as the information is assumed to be easy for most people to answer. However, it is information that is relatively easy for others to find out. The usernames of three friends in the game are requested as most people who play this game have some friends they have been playing with for years. That information should therefore be easy to provide. The usernames of three opponents in the game are harder to provide but for people who mostly play against random players and do not add friends, it is necessary information to request. It is not a requirement that the person making the request gives right answers to all questions, but an assessment is made based on how right or wrong the answer is.

IMY notes that it appears from the material the company has submitted, consisting of the correspondence between the complainant and the company, that the complainant did not withdraw their request for erasure. Furthermore, it appears from the email correspondence, in particular the email sent by the MAG Support Team on 11 March 2021, that the data in question were requested by the company in order to enable the complainant to access the account for the purpose of requesting erasure. The company's claim that the complainant's request for erasure had been changed to a request for access, and that the requested information intended to identify the complainant only in the event of a request for access, can therefore be disregarded. The company has indeed requested further information from the complainant in order to confirm the complainant's identity, however IMY considers that it appears that it is still a request for erasure that the complainant wants to be granted. It also appears that the company requested the information in connection with the complainant's request for erasure.

As regards the information requested by the company from the complainant, IMY states the following. It follows, inter alia, from the EDPB's guidelines on the right of access that the controller must take into account in the proportionality assessment the type of personal data processed (e.g. special categories of data or not), the nature of the request, the context in which the request is made and any harm that may arise as a result of improper disclosure. At the time of the complainant's request, the company processed only one email address associated with the complainant and the advertisingId/vendorId from their telephone, the complainant's username and password. In IMY's view, an erroneous erasure of that information would not have any significant disadvantages or consequences for the complainant. The requirements for identification could thus be set relatively low. Furthermore, it has been shown that correct answers to all the questions were not required and that the identity of the complainant was subsequently confirmed by a different method of identification which required considerably fewer data. Confirmation that it is the complainant's user account sent from the e-mail address linked to the user account was deemed sufficient to confirm the complainant's identity and to comply with the request on 7 November 2022.

IMY therefore considers that, taking into account the nature of the request, the type of personal data processed and the method of identification subsequently used, the data in the form of the usernames of three friends and three opponents cannot be considered necessary or proportionate to confirm the identity of the complainant in accordance with Article 12(6) of the GDPR.

Has the company facilitated the exercise of the right to erasure under Article 12(2) of the GDPR?

The next question is whether it has been compatible with Article 12(2) GDPR to require the complainant to log in their account and make their request from within the game.

In essence, the company stated the following. If the user can respond so well that the company determines that the user owns the account, the support will set the email address for recovery. The user can then set a new password and log in. Since, in the present case, the case had changed to a request for access, the company normally want the user to be logged in to their account in order to exercise their request.

As IMY noted in the section above, it appears from the material the company submitted that the complainant did not withdraw from their request for erasure and that the company requested the data in question in order to enable for the complainant to access the account in order to request erasure from within the game.

The EDPB's guidelines on access state, among other things, that the controller may encourage the data subject to use a self-service tool, but that the controller must also handle requests for access that are not sent through the established communication channel. By requiring the complainant, whose request for erasure has been received by the company, that, after answering questions intended to confirm their identity, they must log in to a game in order to send their request from within the game, the company has not made it easier for the complainant to exercise their right to erasure. IMY therefore considers that the company thereby acted in breach of Article 12(2) of the GDPR.

Has the complainant's request for erasure pursuant to Article 17 GDPR been complied with?

The complaint shows that the complainant requested erasure on 31 January 2021 and that it has not been satisfied at the time of the complaint. The company states that on 7 November 2022, following correspondence with the complainant on 30 October and 6 November 2022, the company erased the complainant's data and the complainant was informed thereof. Since the complainant's request for erasure has now been met, there is no reason to investigate the matter further in that part.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be taken into account when imposing administrative fines and when determining the amount of the fine. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The current supervision covers MAG Interactive AB's handling of an individual complainant's request for erasure and the established infringements are relatively far back in time (2021). MAG Interactive AB has now also fully complied with the complainant's request for erasure. Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that MAG Interactive AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This decision has been taken by the specially appointed decision-maker, legal advisor [REDACTED], following a presentation by legal advisor [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) decision, 2023-05-26 no. IMY-2023-2978. Only the Swedish version of the decision is deemed authentic.

Registration number
IMY-2023-2978 IMI.Case
491994 Complaint, LDA-
1085.310276/20-1.

Date of final decision:
2023-05-26

Date of translation:
2023-03-22

Final decision pursuant to Article 60 under the General Data Protection Regulation — Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that the investigation has not shown that Klarna Bank AB has processed the complainant's personal data in breach of Articles 12(3) and 15 of the General Data Protection Regulation (GDPR)¹ in the manner alleged in the complaint.

The case is closed.

Report on the supervisory report

Processing

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Klarna Bank AB (the company or Klarna) due to a complaint. The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation from the supervisory

authority in (Germany) where the complainant has lodged their complaint in accordance with the GDPR's provisions on cooperation in cross-border processing. The investigation in the case has been carried out through written correspondence. Since this is a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned has been the data protection authorities in Denmark, Germany, Norway, Netherlands, Poland, Italy, Finland and Austria.

Postal adress:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone
08-657 61 00

The complaint

In its complaint, the complainant essentially stated the following. On 9 October 2020,

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).

the complainant requested access to his/her personal data in accordance to Article 15 of the GDPR. The complainant received no information or document from Klarna. The complainant received only one automatic e-mail from Klarna, which contained information that it had received the complainant's e-mail concerning the request for access to her/his personal data.

What Klarna has stated

Klarna Bank AB has mainly stated the following. Klarna is not the data controller for the current processing to which the complaint relates. The request was received by Klarna on 9 October 2020. Klarna has handled the request received and has taken these following steps. On 12 October 2020, Klarna's customer service asked the complainant to add information about his/her identity and requested which of the complainant's e-mail inbox was used for the purchase from Klarna. The complainant has not returned with reply. At the time of the request, Klarna had reason to doubt the complainant's identity and was therefore unable to fulfil his/her's request.

The complainant's request was one of the complaints communicated to Klarna with the supervisory authority in Germany (Berlin) in June to August 2021. In connection with the contact with the he supervisory authority in Germany (Berlin), information was sent to the complainant pursuant to Article 15, by post on 13 August 2021 and Klarna informed the complainant by e-mail the same day.

Klarna considers that information to the complainant has been provided within the specified timeframe in pursuant to Articles 12(3) and 15 of the GDPR after the complainant has provided the necessary information regarding his/her identity.

Justification of the decision

Applicable provisions, etc.

Article 12(3) of the GDPR requires the controller to provide the data subject, upon request, without undue delay and in any event no later than one month after receiving the request, with information on the actions taken pursuant to Article 15. The one-month time limit may be extended by a further two months where the request is particularly complex or the number of requests received is high. If the time limit of one month is extended, the controller shall inform the data subject of the extension.

Notification of the extension of the deadline shall take place within one month of receipt of the request. The controller shall also indicate the reasons for the delay.

Without prejudice to Article 11, where the controller has reasonable grounds to doubt the identity of the natural person making a request pursuant to Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject. This is clear in Article 12(6).

Pursuant to Article 15, the data subject has the right to obtain from the controller a copy of the personal data processed by the controller. The data subject shall also receive other information, such as the purpose for which the personal data are processed and to which recipients or categories of recipients the data are disclosed.

Assessment of the Swedish Authority for Privacy Protection (IMY)

The investigation shows that Klarna Bank AB has started handling the complainant's request for access of personal data within one week of receipt of the request. Klarna has also informed the complainant that the processing of the request for access will commence as soon as sufficient information is received to verify the complainant.

The request was completed on the same day as additional information was received to the company. IMY considers that there has been no reason to question Klarna's information in this part.

IMY considers that the complainant's request has been handled and fulfilled without undue delay within the meaning of Article 12(3) and 15 of the GDPR.

Against this background, IMY notes that the investigation in the case has not shown that Klarna Bank AB has processed the complainant's personal data in breach of Article 12(3) and 15 of the GDPR.

The case is closed.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision in case with national reference number, DI-2019-6696. Only the Swedish version of the decision is deemed authentic

National case number:
DI-2019-6696

Final decision under the General Data Protection Regulation — Spotify AB

Date:
2023-06-12

Table of contents

Decision of the Swedish Authority for Privacy Protection	3
Spotify AB's general procedures for handling access requests.....	3
Examination of individual complaints	3
1 Presentation of the supervisory case.....	5
2 Applicable provisions	6
3 Spotify AB's general procedures for handling access requests - Grounds for the decision.....	7
3.1 Information — Article 15(1)(a) to (h) and (2) GDPR	7
3.1.1 What Spotify AB has stated	7
3.1.2 Assessment by the Swedish Authority for Privacy Protection.....	8
3.2 Right of access to personal data and copy of personal data undergoing processing — Article 15(1) and (3) GDPR.....	12
3.2.1 What Spotify AB has stated	12
3.2.2 Assessment by the Swedish Authority for Privacy Protection.....	15
4 Review of individual complaints — Grounds for the decision	19
4.1 Complaint 1 (from the Netherlands with national reference number z2018-28415).....	19
4.1.1 Background	19
4.1.2 What Spotify AB has stated	20
4.1.3 Assessment by the Swedish Authority for Privacy Protection	21
4.2 Complaint 2 (from Austria with national reference number D130.198).....	22
4.2.1 Background	22
4.2.2 What Spotify AB has stated	23
4.2.3 Assessment by the Swedish Authority for Privacy Protection	24
4.3 Complaint 3 (from Denmark with national reference number 2018-31-1198).....	25

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

5 Choice of corrective measure	26
5.1 Applicable provisions	26
5.2 Same or linked data processing.....	26
5.3 Infringements relating to the information pursuant to Article 15(1) and (2) GDPR and to the description of the data in the technical log files	27
5.4 Infringements relating to complaints 1 and 2	29

Decision of the Swedish Authority for Privacy Protection

Spotify AB's general procedures for handling access requests

The Swedish Authority for Privacy Protection finds that, during the period from 16 November 2021 to 16 May 2022, in the information to be provided pursuant to Article 15(1) and (2) of the General Data Protection Regulation (GDPR)¹, Spotify AB (556703-7485) did not provide sufficiently clear information on:

- the purposes of the processing;
- the categories of personal data concerned;
- categories of recipients of the personal data;
- the envisaged period for which the personal data will be stored or, if not possible, the criteria used to determine that period;
- the source of personal data;
- appropriate safeguards when personal data are transferred to third countries.

The Swedish Authority for Privacy Protection further finds that Spotify AB, during the period from 11 June 2019 to 16 May 2022, by providing by default the description of the data in the technical log files in English, has not complied with the requirement that all communications provided to the data subject pursuant to Article 15 of the GDPR shall be clear and intelligible as set out in Article 12(1) of the GDPR.

Spotify AB has thus processed personal data in breach of Articles 12(1), 15(1)(a) to (d), 15(1)(g) and 15(2) of the GDPR.

Pursuant to Articles 58(2) and 83 of the GDPR, the Swedish Authority for Privacy Protection decides that Spotify AB shall pay an administrative fine of 58,000,000 (fifty-eight million) SEK for these infringements.

Examination of individual complaints

The Swedish Authority for Privacy Protection finds with regard to complaint 1 that in its handling of the complainant's request for access made on 27 May 2018, Spotify AB has processed personal data in violation of:

- Article 12(3) of the GDPR, by late submission of the copy of personal data;
- Articles 12(1), 15(1) and 15(3) of the GDPR, by not having provided all the complainant's personal data in an intelligible form in the copy of personal data provided by Spotify AB.

The Swedish Authority for Privacy Protection finds with regard to complaint 2 that in its handling of the complainant's request for access made on 10 October 2018, Spotify AB has processed personal data in violation of:

- articles 15(1) and 15(3) of the GDPR, by not having given access to all personal data that Spotify AB processed about the complainant in the copy of personal data provided by Spotify AB;

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).

- articles 15(1)(a) to (h) and 15(2) GDPR, by not providing any of the information specified in these provisions.

The Swedish Authority for Privacy Protection issues a reprimand to Spotify AB pursuant to Article 58(2)(b) of the GDPR for the infringements relating to complaints 1 and 2.

Pursuant to Article 58(2)(c) of the GDPR, the Swedish Authority for Privacy Protection orders Spotify AB to comply with the complainant's request for access in respect of complaint 2. This is done by providing the complainant access to all personal data that Spotify AB processes regarding the complainant, with exception for information which is subject to any applicable derogation provided for in Article 15(4) of the GDPR and Chapter 5 of the Data Protection Act², by providing the complainant with a copy of the personal data pursuant to Article 15(3) of the GDPR and provide information pursuant to Articles 15(1)(a) to (h) and 15.2 of the GDPR. This measure shall be implemented no later than one month after this decision has become final.

² Act containing supplementary provisions to the EU General Data Protection Regulation (SFS 2018:218).

1 Presentation of the supervisory case

Due to complaints that the Swedish Authority for Privacy Protection (IMY) has received against Spotify AB regarding the right of access pursuant to Article 15 of the GDPR, IMY has initiated supervision against Spotify AB in order to investigate whether Spotify AB's way of handling the data subject's request for access is in accordance with the provisions of the GDPR. IMY has initially examined Spotify AB's general procedures when handling access requests and not the circumstances in the individual complaints. The investigation has focused on whether Spotify AB's processes and procedures for providing access under Article 15 of the GDPR generally enable data subjects to access the personal data Spotify AB processes about them and other information under the provision. In this context, "data subject" refers to customers who use Spotify AB's services and no other categories of data subjects, e.g. employees of Spotify AB.

IMY has not, in this investigation, verified what personal data Spotify AB processes and whether all these are disclosed at each individual request. For example, no comparison has been made between Spotify AB's records of processing pursuant to Article 30 of the GDPR and the personal data contained in the copy of personal data pursuant to Article 15(3) of the GDPR. In the context of this investigation, IMY has also not examined whether Spotify AB's personal data processing otherwise complies with the provisions of the GDPR, e.g. regarding principles and legal basis for the processing.

IMY initiated the supervisory case by sending a questionnaire on 11 June 2019. Reply to the questionnaire was received on 31 July 2019. On 16 October 2019, a request for additional information on the case was sent to Spotify AB. A reply was received on 15 November 2019. Spotify AB has subsequently submitted further additions on 25 August 2020 on its own initiative in order to inform IMY of updates regarding procedures for handling requests for access.

Spotify AB is an organisation with operations and users in several EU Member States. Due to the cross-border nature of the case, IMY has applied the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. All data protection authorities in the EU have been concerned supervisory authorities in this case. With regard to the cooperation and consistency mechanisms, and the need for harmonised complaint handling within the EU³, IMY extended in November 2020 the ongoing general oversight to cover also the three individual complaints, which also include the complaints which initially led to the investigation of the general procedures.

On 5 November 2020, IMY requested Spotify AB to state its position on the infringements alleged in the complaints and what measures Spotify AB had taken to respond to the respective requests for access. Spotify AB replied to IMY's request on 18 December 2020. Spotify AB subsequently submitted additional information, on 15 April 2021 in response to additional questions sent by IMY on 24 March 2021 and 31 August 2021 in response to questions sent by IMY on 9 July 2021.

On 19 October 2021, a further request for additional information was sent regarding Spotify AB's general procedures. A reply was received on 12 November 2021. On

³ In 2020, DPAs worked jointly to establish common approaches to the handling of complaints, resulting in an internal guidance established in February 2021. From the fact that the authority previously used complaints to identify recurring patterns and risks, but as a general rule closed the complaints with a standard response, IMY now makes an individual assessment of each complaint. Internal EDPB Document 02/2021 on SA's duties in relation to alleged GDPR infringements, adopted 2 February 2021.

June 8 and October 17, 2022, Spotify AB has, on its own initiative, submitted further additions in order to inform IMY of updates regarding their procedures for handling requests of access.

Spotify has expressed its views on IMY's draft decision on 20 December 2022. IMY then gave the concerned supervisory authorities the opportunity to give their opinion in accordance with Article 60 of the GDPR. The French Data Protection Authority has raised a relevant and reasoned objection to the IMY's draft decision. Spotify has been given the opportunity to comment on the objection on 13 March 2023 as well as on the revised draft decision shared by IMY. Spotify's response was received on 11 April 2023.

Hence, as described above, the supervisory case consists of an investigation of Spotify AB's general procedures for handling requests of access and, also, an investigation of what has occurred in the three complaints. The general procedures that Spotify AB used to provide personal data pursuant to Article 15(1) and (3) of the GDPR covered by IMY's supervision where those in force from the start of IMY's supervision on 11 June 2019 until 16 May 2022. As regards the information pursuant to Article 15(1) and (2) of the GDPR to be provided in the event of a request of access, Spotify AB has updated it several times since the start of IMY's supervision. IMY has therefore limited its investigation to the information provided during the period from 16 November 2021 to 16 May 2022.⁴

2 Applicable provisions

Pursuant to Article 15(1) of the GDPR, the data subject has the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed and, if so, to have access to the personal data and the following information:

- a) The purposes of the processing;
- b) The categories of personal data concerned;
- c) The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- d) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- e) The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- f) The right to lodge a complaint with a supervisory authority;
- g) Where the personal data are not collected from the data subject, any available information as to their source;
- h) The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

⁴ See Spotify AB's information pursuant to Article 15 of the General Data Protection Regulation in Annex 2. The information, which was downloaded by IMY on 16 May 2022, shows that the current website was last updated on 16 November 2021. The period of investigation is therefore set at the period from 16 November 2021 to 16 May 2022.

Article 15(2) of the GDPR states that where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

It follows from Article 15(3) of the GDPR that the controller shall provide the data subject with a copy of the personal data undergoing processing. Furthermore, where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided, in a commonly used electronic form.

Recital 63 of the GDPR states, as far as relevant, that:

A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. (...) Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. (...)

In addition, it follows from Article 12(1) of the GDPR that the controller shall take appropriate measures to provide any communication under Article 15 to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

It follows from Article 12(2) of the GDPR that the controller shall facilitate the exercise of the data subject's right of access under Article 15.

Pursuant to Article 12(3) of the GDPR, the controller shall provide information on action taken on a request under Article 15 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

3 Spotify AB's general procedures for handling access requests - Grounds for the decision

3.1 Information — Article 15(1)(a) to (h) and (2) GDPR

3.1.1 What Spotify AB has stated

Spotify AB has stated the following. Spotify AB provides information in accordance with Article 15(1)(a) to (h) and Article 15(2) GDPR via an online function. This feature is available in 21 different languages and visitors will automatically be given information in languages based on language settings in their browser.

Data subjects exercising their right of access are informed of the function in several ways. Each copy of personal data provided pursuant to Article 15(3) GDPR includes a hyperlink to the information. The information can also be found online, partly in the list

of available features on Spotify AB's "*Privacy & Security*" page, partly via the answer to the question "Where can I find information about Spotify AB's processing of personal data that Spotify AB is obliged to provide pursuant to Article 15 of the GDPR?" on Spotify AB's "*data rights and privacy settings*" page.

In the information⁵ pursuant to Article 15 of the GDPR provided by Spotify AB during the period from 16 November 2021 to 16 May 2022, Spotify AB provided, inter alia, information on the purpose of processing (Article 15(1)(a)), the categories of personal data processed (Article 15(1)(b)), recipients or categories of recipients (Article 15(1)(c)) and the source of the personal data (Article 15(1)(g)). In addition, the Article 15 information also included information on international transfers (Article 15(2)), the criteria for the retention of personal data (Article 15(1)(d)), the rights of the data subject (Article 15(1)(e)), the right to lodge a complaint with the data protection authority (Article 15(1)(f)), automated decision-making (Article 15(1)(h)) and the possibility of obtaining a copy of personal data.

In the information pursuant to Article 15 of the GDPR, Spotify AB also informed that the processing of personal data is described in more detail in Spotify AB's privacy policy, which could also be accessed through a direct link. The privacy policy contains, among other things, descriptions of the categories of personal data that Spotify AB processes.

Spotify AB has stated that all questions that are not answered by the information pursuant to Article 15 of the GDPR or which have not been explained to the user are promptly escalated to Spotify AB's data protection team. In this way, Spotify AB states, the data protection team becomes aware of, and is given the opportunity to answer, questions about clarifications or requests for more individualised information about the processing of personal data pursuant to Article 15 of the GDPR.

3.1.2 Assessment by the Swedish Authority for Privacy Protection

IMY notes that Spotify AB's function for information pursuant to Article 15 of the GDPR during the period under review was available on several pages on Spotify AB's website. Furthermore, a link to the information was included in the "*Read me first*" file attached to each copy of personal data provided to the data subject in accordance with Article 15(3) GDPR upon a request of access. In view of the above, IMY considers that Spotify AB's procedures during the current period were sufficient to ensure that information pursuant to Article 15 was provided to the data subject at any request for access.

IMY further notes that Spotify AB's information pursuant to Article 15 of the GDPR covered all items of information that pursuant to Article 15(1)(a) to (h) and (2) of the GDPR are to be provided to the data subject. However, in order for the information to meet the requirements of the GDPR, the information must also be designed in such a way that the purpose of the right of access is fulfilled.

The purpose of the right of access is for the data subject to be aware that processing is taking place and to be able to verify that it is lawful, as stated in recital 63 of the GDPR. For example, a data subject should be able to check which categories of data are processed about him or her, for what purposes and for how long. In order for the data subject to verify the lawfulness of the processing of personal data, he or she must know which processing operations are relevant in his or her particular case. The

⁵ See Annex 2

information provided in this respect must be provided in a manner that meets the transparency requirements of Article 12(1) of the GDPR.

In light of the purpose of the right of access, there is often a need to adapt the content of the information under Article 15(1) and (2) of the GDPR to the data subject who has made the request, for example depending on which of the controller's services the data subject has chosen to use. However, this does not apply to all parts of the information. While the right to lodge a complaint with a supervisory authority (Article 15(1)(f) GDPR) does not change depending on who requests access, other data may vary depending on the service the data subject uses, such as which categories of personal data are processed, recipients and where personal data were collected. The same applies to information on whether a transfer has taken place to a third country and, if so, what appropriate safeguards have been taken during the transfer.

Therefore, in order for the data subject to be able to verify that the processing concerning him or her is lawful, it is necessary, in accordance with the above, that Spotify AB shall have taken steps to adapt the information to the specific situation of the data subject.⁶

IMY notes that the information provided⁷ by Spotify AB pursuant to Article 15 of the GDPR was provided in general terms. The same information was thus provided regardless of who requested access under Article 15 of the GDPR. The information was therefore not adapted on the basis of every request of access. However, Spotify AB described when certain information was relevant to the data subject, such as "*If you use a third party service (...)*", "*If you choose to pay for a service or function by invoice (...)*" and "*In cases where you have given us permission (...)*". There were thus some abilities for the data subject to determine which information was related to him or her. There was also a possibility for data subjects to turn to Spotify AB and request more individualised information as well as clarifications of the information provided.

IMY believes that such information provided in general terms may be appropriate for standardised services involving personal data processing. However, in order for data subjects to understand how their personal data are processed, it must always be possible to clearly and easily determine which information is applicable in which situations based on the information provided. This means that the possibility for the data subjects to turn to Spotify AB for more individualised information as well as clarifications do not affect the assessment of whether the information is sufficiently clear in this respect. Generally drafted information shall not give rise to any ambiguity as to whether the data subject is concerned by the information in question or not based on his or her individual situation. IMY therefore has to examine whether the information provided by Spotify AB met these requirements.

Information on categories of personal data, purposes, recipients and source

Information about the purposes of the processing shall relate to the purposes for which the data subject's personal data are actually processed, and may not consist merely of a list of different purposes, without clarification what purposes relates to the person requesting access. Furthermore, information on the categories of personal data processed may need to be adapted to the circumstances of the data subject requesting access. As regards the information of recipients or categories of recipients,

⁶ Cf. European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, version 2.0 (adopted on 28 March 2023), paragraph 113.

⁷ See Annex 2

such information should be as specific as possible. The controller should normally state the actual recipients to whom the personal data have been or are to be disclosed, unless this is impossible because, for example, there is not yet information on who the recipients are. In addition, all available information as to their source of the personal data shall be provided if the personal data have not been collected from the data subject.⁸

As regards the information provided by Spotify AB about the purposes of the processing, recipients of personal data and the source from which the data were collected, IMY notes that the information was divided into different categories of personal data. Those categories of personal data consisted of '*user data*', '*use data*', '*plan verification data*', '*voice data*', '*payment data*' and '*competition, survey and lottery data*'. The categories of personal data provided were generally held and, in several cases, for example, in relation to "*user data*" and "*use data*" did not contain any further description of which personal data could be included. IMY considers, especially given the absence of a clear description of the categories in question, that it was not possible for data subjects to understand, on the basis of the information provided, which personal data were included in the different categories. Since the information on purposes, recipients and source was divided into those categories of personal data, this shortcoming had the effect that it was also not possible for data subjects to easily understand which personal data were processed for what purposes, which personal data were obtained from what source or which personal data were provided to a particular recipient or category of recipients. Data subjects have thus not been able to determine how their personal data were processed.

IMY therefore considers that Spotify AB has not provided sufficiently clear information about the purposes of the processing (Article 15(1)(a) GDPR), the categories of personal data concerned (Article 15(1)(b) GDPR), recipients or categories of recipients (Article 15(1)(c) GDPR) or the source from which the data were collected (Article 15(1)(g) GDPR). The information was not concise, and transparent, nor easily accessible. It therefore did not meet the requirements of Article 12(1) of the GDPR.

Information about the retention period

Information provided on how long personal data is stored shall be sufficiently specific to enable the data subject to understand how long his or her personal data will be stored. If it is not possible to specify the envisaged period for which the data will be stored, the relevant event affecting that period should instead be specified, such as the expiry of a guarantee period. The retention periods shall relate to the personal data relating to the data subject requesting access. Where these personal data are subject to different retention periods, information on the retention periods shall be given in relation to each relevant data processing and category of personal data.⁹

Spotify AB provided information on retention periods under the heading "Criteria for the retention of personal data". The information contained general information about the purposes for which the personal data are stored and the criteria used to determine the retention periods. It was stated, inter alia, that personal data is retained by default for 90 days, unless a longer period is chosen due to a legitimate business reason. In addition, it was stated that personal data is stored for an appropriate period to deliver a

⁸ Cf. European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, version 2.0 (adopted on 28 March 2023), point 114-120 and the judgement of the CJEU on 12 January 2023 in Case C-154/21 Österreichische Post.

⁹ European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, version 2.0 (adopted on 28 March 2023), paragraph 118.

personal service over time and that streaming history is usually retained over the lifetime of an account.

The information on how long data is retained was provided in general terms and, with the exception of, *inter alia*, the information on streaming history, not clearly linked to the categories of personal data covered by the different retention periods. The data subjects were therefore unable to determine which of their personal data was retained for what period of time. Furthermore, the criteria for determining the retention period set out in the information were, in some cases, very imprecise. For example, it is difficult for a data subject to understand what was included in "legitimate business reasons" and thus in what situations personal data was retained for more than 90 days or what it meant that streaming history was "usually" kept over the lifetime of an account.

In an overall assessment, IMY considers that the information provided concerning retention periods did not meet the requirements of Article 15(1)(d) of the GDPR, both because the information in this part was set out in general terms and not related to the relevant category of personal data, and partly because some of the criteria used to determine the retention period were too imprecise to enable the data subject to understand how long his or hers personal data were stored. The information was not concise and transparent, nor easily accessible. It therefore did not meet the requirements of Article 12(1) of the GDPR.

Information on third country transfers

In order for the data subject to be able to assess whether a possible transfer of his or her personal data to a third country is lawful, the data subject must be provided with meaningful information enabling it to be ascertained whether his or her personal data have been transferred and, if so, what safeguards have been used. In order to enable the data subject to verify whether his or her personal data have been lawfully processed, the information should normally also state to which third countries the transfer has taken place.¹⁰

The information provided by Spotify AB regarding transfers to third countries under the heading "*International Transfers*" showed that Spotify AB may share personal data globally with other companies in Spotify Group, service providers, partners, etc. Furthermore, it was stated that Spotify AB ensures that the transfer is carried out in accordance with applicable data protection and confidentiality laws and that technical and organisational measures, and in particular appropriate safeguards, are applied, such as the standard contractual clauses approved by the European Commission when personal data are transferred from the European Economic Area (EEA).

IMY notes that the information provided by Spotify AB regarding third country transfers was given in general terms and not linked to the data subject's own situation. In that regard, it was not clear whether the personal data of the data subject had been transferred to a third country and, if so, what appropriate safeguards had been taken during the transfer. In addition, it was not clear to which third countries transfers had taken place. IMY therefore considers that the information provided regarding third country transfers did not meet the requirements of Article 15(2) GDPR. The

¹⁰ Cf. Article 29 Guidelines on Transparency under Regulation (EU) 2016/679, WP260rev.01, adopted by the European Data Protection Board, p. 40

information was not concise and transparent, nor easily accessible. It therefore did not meet the requirements of Article 12(1) of the GDPR.

Summary assessment of the information pursuant to Article 15(1) and (2) GDPR

In conclusion, IMY finds that the information provided by Spotify AB pursuant to Article 15(1) and (2) of the GDPR during the period from 16 November 2021 to 16 May 2022 has been deficient in the above-mentioned respects. Spotify AB has thus processed personal data in breach of Articles 12(1), 15(1)(a) to (d), 15(1)(g) and 15(2) of the GDPR.

3.2 Right of access to personal data and copy of personal data undergoing processing — Article 15(1) and (3) GDPR

3.2.1 What Spotify AB has stated

Spotify AB has stated that its response to the request for access, with a few exceptions, is designed to disclose all personal data that they process in relation to the data subject. Spotify AB has also set out its procedures to ensure that all personal data is disclosed, for example in the event of new or updated personal data processing.

The copy of personal data provided by Spotify AB pursuant to Article 15(3) of the GDPR can be provided through three different replies, Type 1, Type 2 and Type 3.

The personal data covered by Type 1 are profile information and the personal data that Spotify AB has deemed to be of the greatest interest to the data subjects. Type 1 therefore includes the data subject's playlists, streaming history and searches from the last year, items saved in the data subject's library, the number of followers the data subject has, the number of users the data subject follows, the names of artists the data subject follows, user data and payment information. In order to provide the data subject with access to Type 1 information, Spotify AB has introduced a feature called "*Download Your Data*" on a website for privacy settings. The website through which the data subject can access this information is accessible to all customers through their Spotify account and is provided in the same language as their Spotify Service. Data subjects will have access to Type 1 information within about seven days. Data subjects can also access the Type 1 information by contacting Spotify AB's customer service.

Type 2 information consists of technical log files stored in Spotify AB's systems linked to the data subjects' user IDs. In order to access the Type 2 information, the data subject may send a request via Spotify AB's web form for privacy matters or by contacting customer service or Spotify AB's data protection officer through any other channel (e-mail, Facebook, Twitter or letter). It takes about two to four weeks to compile and provide this personal data.

Type 3 information is the information that a data subject specifically requests and may, for example, relate to the data subject's listening history at a certain date, an extended listening history or a request for unstructured personal data, such as a request for a particular email correspondence. Type 3 information can be requested in the same way as Type 2 and such a request normally takes less than 30 days to process. In case it takes longer to process the request, due to the complexity of the request, the data subject is informed of the delay.

On June 15, 2021, Spotify AB has implemented changes whereby all Spotify users who request a copy of personal data, in addition to what is available in the “*Download Your Data*” tool, or who directly request a copy of all their personal data from Spotify AB’s customer service, will have access to extended streaming history as well as technical log file provided in one package.

Spotify AB has stated that the design of the process and its development to date are a combined result of joint discussions, careful consideration and analysis, as well as meetings with the relevant customer service and development teams. Spotify AB’s data protection team has provided advice on legal requirements and best practices in data protection and continues to update these on the basis of a number of identified parameters, including relevant and up-to-date legislation, guidelines, the ability to quickly respond to a large number of requests, user-friendliness and categories of personal data processed.

Spotify AB has stated that it has over 232 million active users per month and that during the period from 25 May 2018 to 30 June 2019, they responded to 753 575 requests for access. According to Spotify AB, the division of data into three different types has made it possible to provide a quick and easy way for the data subject to download the personal data likely to be most relevant to the data subject and to generate responses on a large scale and with the speed required to satisfy the majority of the data subjects.

Furthermore, Spotify AB refers to statements in the EDPB’s transparency guidelines¹¹ that there is an inherent tension in the GDPR between the requirements to provide data subjects with comprehensive information on the one hand and that the information should be provided in a concise, clear, intelligible and easily accessible form, on the other hand, the need to determine how to prioritize information that must be given to data subjects, and what levels of detail and methods are appropriate for conveying the information, and that the principle of transparency is an overarching obligation. Spotify AB considers that these guidelines are relevant to the design of a concise, transparent, easily understandable and easily accessible process for data subjects to exercise their rights under Article 15 of the GDPR. By providing three layers of responses to the request of access to data subjects, Spotify AB intends to balance the interests of the GDPR correctly for the benefit of Spotify AB’s data subjects. Spotify AB’s objective is to provide accurate information in accordance with Article 15 to all data subjects at the right time by providing information in different layers and in different ways.

Spotify AB states that it informed data subjects that it was possible to request access to more personal data than those covered by Type 1 and Type 2, and that this information was provided to data subjects before requesting access to their personal data. Furthermore, Spotify AB stated that it was clear that data subjects could request access to more personal data than those covered by Type 1 by requesting a Type 2 response. In addition, data subjects could contact Spotify AB’s customer service with specific requests (so-called Type 3 request). The information about this is provided in various ways, including on the “Personal data rights and privacy settings” website and on the website where information pursuant to Article 15 of the GDPR is published. Furthermore, when a user requests access to the personal data covered by Type 1 by accessing “Download Your Data”, it is clear from the context that users have access to a selection of their personal data and not all of their personal data. The “Download your data” page also contains a reference to the website “Personal data rights and

¹¹ Article 29 Working Party’s *Guidelines on Transparency under Regulation (EU) 2016/679*, WP260rev.01, adopted by the European Data Protection Board, paragraphs 1 and 34.

privacy settings". In case of requests under both Type 1 and Type 2, information is provided in accordance with Article 15 of the GDPR, which contains a comprehensive description of the available data. The sources of information also explain that the user can request access to their personal data via customer service or by contacting Spotify AB via email. If a user contacts Spotify AB's customer service to exercise the right of access pursuant to Article 15 of the GDPR, customer service can explain all three types of personal data available and inform users of the additional information available. The data subjects were also informed that they could request access to more personal data than they have already downloaded on the website "Understand my data".

In addition, during the course of the case, Spotify AB has updated the information addressed to the data subjects in order to make it more transparent for data subjects that there is more to request than is available in the "*Download your data*" tool.

With regard to the clarity of the information, Spotify AB has stated, in essence, the following. In designing the format for responding to access requests, Spotify AB focused on providing all information in a way that makes it relevant, transparent and helpful to the data subjects. Spotify AB developed a procedure to ensure that the descriptions of the personal data are accurate and complete, which included extensive efforts to translate technical information into a simple language that can be understood by an average customer, without removing the details required for transparency. In order to facilitate understanding, Spotify AB does, among other things, the following.

- When downloading Type 1 information, the data subject also receives a so-called "*Read Me First*" file. The "*Read Me First*" file contains a link to the website "*Understanding My Data*", which describes the format and personal data included in Type 1. This page has been updated during the course of the case to include a general description of the data in the technical log files and the extended streaming history. The linked pages are automatically displayed in the customer's preferred language based on the language setting in the customer's browser.
- Type 2 information, which consists of technical log files¹², contains some information that is highly technical in nature. In order to help data subjects understand the formatting of the personal data, Spotify AB provides a detailed description of the personal data in a specific file together with the data provided (in a "*Read Me First*" file for the Type 2 request). This description is provided by default in English. Spotify AB also answers customer questions about the substance of the personal data provided, as part of its process for data subjects' requests of access. Furthermore, Spotify AB continuously updates both the format of technical log files related to the customer's user ID (Type 2) and the corresponding information in the Type2 "*Read Me First*" file to increase transparency based on the questions asked.
- In the case of special enquiries (Type 3), when the personal data provided may require explanations, Spotify AB may, if necessary, provide the information in an email to the data subject together with the copy of the personal data.

Spotify AB has stated the following as a background to the fact that the description of the Type 2 data by default is provided in English. To ensure that the information provided by Spotify AB to the data subjects is correctly translated into their local language, the files to be translated in manual translation are sent to professional translators. Given that technical log data changes more dynamically over time than other personal data collected, Spotify AB would have to send the comprehensive "*Read me First*" file for translation several times a month. This would be disproportionate and unreasonable to do for all local languages given the extra time,

¹² From 15 June 2019, the Type 2 information includes, in addition to the technical log files, extended listening history.

resources and administration it would entail. Furthermore, many of the words that appear in the technical log data do not typically have a translation because they often reflect technical concepts that are mainly communicated in English and are usually not translated into local languages. However, Spotify AB helps to translate the information into local language if a user requests it to the extent that the technical terms are possible to translate. Spotify has also stated that it has responded to approximately 340 000 requests for access to technical log files. Of those requests, only two data subjects have turned to the company and requested a translation of the description into their local language. Spotify further argues that translation of the technical log files without a request would mean that all data subjects would have to wait longer for their right to access the technical log files to be satisfied.

Regarding the format used, Spotify AB has stated that the personal data is provided in JSON format, which according to Spotify AB is a structured and commonly used format that can be understood by both computers and people. However, data provided as a result of a Type 3 request is provided in the format necessary to respond to the request.

On October 17 2022, Spotify AB informed IMY that Spotify AB has since that time enabled data subjects to request access to account data, extended streaming history and technical log files directly through the “Download Your Data” tool, i.e. without contacting customer service. These procedures are not subject to IMY’s review as the update has taken place after 16 May 2022.

3.2.2 Assessment by the Swedish Authority for Privacy Protection

Pursuant to Article 15(1) of the GDPR, the data subject has the right to obtain confirmation as to whether the controller processes personal data concerning him or her and, if so, to have access to the personal data. The controller is obliged, pursuant to Article 15(3), to provide the data subject with a copy of the personal data undergoing processing. The right of access is the same regardless of who the controller is, but the way in which a request of access is handled may vary, depending, *inter alia*, on the amount of the personal data processed and the number of data subjects. Pursuant to Article 12(2) of the GDPR, the controller has an obligation to facilitate the exercise of the data subject’s rights.

The purpose of the right of access is to make the data subject aware of the processing carried out and to be able to verify that it is lawful. The controller must therefore ensure that the copy of personal data provided contains all the personal data processed about the data subject and is presented in a way that is comprehensible to the data subject. Access to personal data must be provided in a manner that meets the transparency requirements set out in Article 12(1) of the GDPR.

The requirements for the presentation and content of the copy means that controllers who process a large amount of data or data which are particularly difficult to understand may need to take specific measures when the information is presented to data subjects.

Spotify AB, whose personal data processing is both extensive and complex, has developed special procedures for handling access requests. The question is whether these procedures enable Spotify AB to provide access to the personal data they process in a way that satisfies the data subject’s right of access.

Dividing the copy of personal data into different layers

Spotify AB divides the copy of personal data into different layers, Type 1, Type 2 and Type 3.

IMY considers that there is nothing that prevents dividing the copy of personal data as long as the right of access is satisfied. On the contrary, it may, in certain situations, make it easier for the data subject to comprehend the information if it is presented in layers, at least in the case of a large amount of information. However, providing the copy of personal data in different layers must neither restrict the right of access nor complicate the exercise of the right of access. The controller must therefore take this into account when assessing whether dividing the copy of personal data is an appropriate measure.

A data subject who turns to a controller to request access to his or her personal data normally lacks knowledge of which personal data are actually processed. Instead, acquiring this knowledge is often the very purpose of the request. If, in this situation, the controller only provides the data subject with a selection of his or her personal data, the data subject may be led to believe that the copy provided is complete.

For this reason, IMY considers that the controller, in the channel it has established in order for the data subject to request access, must be clear that the copy of the personal data is divided into different layers. It shall also be clear to the data subject what information is contained in the various layers and how the data subject can access them.¹³

Spotify AB has stated that the data subject, in several different channels, receives information that access to different personal data can be requested in different ways. These channels show that access to "*your most relevant personal data*" can be obtained through the "*download your data*" function and that access to technical log files, extended streaming history or responses to other specific data protection requests can be obtained upon request via email or customer service. IMY can, from the examples set out in Spotify AB's statement, note that the information provided to data subjects also contains an overall list of the personal data covered by the different types of requests.

IMY considers that the information provided by Spotify AB in this regard, during the period covered by the review of the general procedures, is sufficiently clear to enable the data subject to understand how the copy is divided, including what data are contained in the different layers, and how the different layers can be requested.

Setting up specific conditions for the exercise of the right of access without it being specifically regulated in the GDPR risks causing the data subject to be unduly hindered in exercising their right. In other words, it may be unnecessarily difficult to exercise the right, which in turn may result in the data subject refraining from requesting all data to which the data subject is entitled. There is reason to underline that, according to Article 12(2) GDPR, the controller has an obligation to facilitate the exercise of the data subject's rights. Therefore, in order to ensure that providing the copy of personal data in different layers does not result in the restriction of the right or that the exercise of the right is hindered, IMY considers that the data subject cannot be required to return to the controller on several occasions in order to have access to all personal data. Nor should it be complicated to request access to the various layers. IMY therefore considers that the data subject should be able to request access to all

¹³ Cf. European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, version 2.0 (adopted on 28 March 2023), paragraph 146.

layers from the outset and that access to them should be easy. Notwithstanding that the data subject, knowing how the data is divided, can still choose to request access to only one or more layers.¹⁴

Spotify AB's statement shows that the data subject can request access to the different layers in different ways. It is not necessary for the data subject to return to Spotify AB in order to access the various layers. However, the data subject may need to take several steps to access multiple layers, e.g. by both downloading Type 1 information through the "*download your data*" function and by requesting access to Type 2 and Type 3 information through customer service. If the data subject addresses the request directly to customer service, the data subject may request access to all personal data at the same time.

IMY considers that the fact that the data subject must take different measures to request the different layers of data may cause some inconvenience. However, the data subject has the possibility to take all these at one time. In addition, all measures can be easily taken through Spotify AB's website. In an overall assessment, IMY considers that Spotify AB's procedures enable the data subject to request access to all his or her personal data in a sufficiently simple manner.

The presentation of the copy and the format of the copy

It follows from Article 12(1) of the GDPR that the information provided under Article 15 of the GDPR must be provided in a concise, transparent, intelligible and easily accessible form using clear and plain language. The requirements for transparency in the individual case must be assessed in the light of the purpose of the right of access, i.e. that the data subject should become aware of the processing carried out and be able to verify the lawfulness of the processing.

Most of the data that Spotify AB processes, especially when it comes to data in the technical log files, is by its nature very technical because it contains e.g. codes and numbers. For an average data subject, such data may be difficult to understand. IMY considers that, providing such information without further explanation would not meet the requirements of transparency, with regard to the purpose of the right. However, since the data to be provided under Article 15(1) of the GDPR and covered by a copy under Article 15(3) of the GDPR shall be the personal data processed, it is not permitted for the controller to modify difficult personal data in order to facilitate understanding. Such information may need to be explained instead.

Spotify AB provides further descriptions, together with the copy of personal data, in order to make the data in the different layers understandable to the data subject. Spotify AB also answers the data subject's questions about the substance of the personal data provided and updates its general procedures and descriptions based on the questions asked.

IMY considers that the data in the technical log files provided by Spotify AB may be complicated to understand, despite the descriptions provided by Spotify AB. However, IMY considers that Spotify AB, by providing these descriptions, enables the data subject, albeit with a certain amount of effort, to assimilate the information. The fact that some effort may be required by the data subject to understand certain particularly

¹⁴ Cf. European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, version 2.0 (adopted on 28 March 2023) paragraph 146.

complex data, despite these descriptions, is a natural consequence of the nature of those data.

By default, Spotify AB provides only the granular description of the data contained in the technical log files in English. Neither Article 12(1) nor Article 15 of the GDPR contains an explicit requirement as to the language or description of personal data to be provided to the data subject. However, IMY considers that it follows from the purpose of the right of access and the requirements for transparency set out in Article 12(1) that data subjects should be able to obtain the information in a language they know, at least when the controller directs its activities to countries where it constitutes an official language.¹⁵ This means that the controller must take sufficient steps to ensure that the data subject understands the information.

Spotify AB provides the predominant proportion of information provided to data subjects under Article 15 of the GDPR based on the language settings of the individual's web settings, i.e. the local language. This includes a general description of the content of the technical logfiles. Furthermore, in the "Read Me First" file provided at each request for access, Spotify provides clear information, in the local language, on the possibility to request a translation of the description of the technical log files. This information is also provided in the local language on the website "Understanding my data". Spotify AB has thus taken extensive measures to provide information in a language that the data subject should be able to understand. However, it has reported significant difficulties in translating the description of the data contained in the technical log files into all the local languages of the countries to which it directs its activities. The difficulties stem from the constant changes in the data in the technical log files and the fact that many technical concepts are difficult to translate from English.

However, IMY notes that Spotify has stated that, at the request of a data subject, it has the possibility to translate the description of the data in the technical log files into a local language to the extent that the technical terms are translatable. As a translation is therefore possible in practice, IMY considers that such a translation should be available even before a request for translation has been made by a data subject. Spotify's stated difficulties in translating the description, including the fact that translation may need to be done on several occasions each month and the additional resources this requires, cannot justify that the description by default is being provided in English. Having regard to the purpose of the right of access, it is essential that the data subject understands which of his personal data have been processed in the technical log files, which presupposes an intelligible description of its content. IMY therefore considers that Spotify should have provided the description in the requester's local language already when the technical log files were provided to the data subject, at least to the extent necessary for the understanding of the data in the technical log files.

In view of the above, IMY considers that Spotify has not taken sufficient measures to ensure that the data subject understands the description of the data in the technical log files when this information is provided by default only in English. Therefore, the information provided by Spotify in this part did not meet the requirement that all communications provided to the data subject pursuant to Article 15 of the GDPR should be clear and intelligible in the manner set out in Article 12(1) GDPR. The fact

¹⁵ Cf. Article 29 Guidelines on transparency under Regulation (EU) 2016/679, WP260rev.01, adopted by the European Data Protection Board, paragraph 13 and the European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, version 2.0 (adopted on 28 March 2023) paragraph 142.

that a data subject has the opportunity to return to Spotify to request a translation does not compensate this deficiency.

It follows from Article 15(3) of the GDPR that a data subject who makes a request for access in electronic form shall receive the information in an electronic format that is commonly used, unless the data subject requests otherwise. Spotify AB provides the information in JSON format. The Guidelines on the right to data portability provide JSON format as an example of a commonly used open format.¹⁶

IMY notes that the requirements for format are different for the right to data portability and the right of access as data portability also requires the data to be provided in a structured and machine-readable format pursuant to Article 20(1) of the GDPR. In light of the purpose of the right of access, IMY considers that the format in which the data is provided under Article 15 of the GDPR must be readable to a natural person. However, there is nothing to prevent the format from being machine-readable as well. Such a format can in many cases make it easier for the data subject to make various compilations or comparisons himself in order to facilitate understanding. IMY considers that JSON format, which can be read by both computers and natural persons, is currently an electronic commonly used format within the meaning of Article 15(3) GDPR.

Summary assessment regarding the right of access to personal data and copy of personal data undergoing processing — Article 15(1) and (3) GDPR

In conclusion, IMY finds that Spotify AB's way of dividing the copy of personal data into different layers does not complicate the exercise of the data subjects' rights and is therefore in compliance with Article 12(2) of the GDPR and that the presentation and format of the copy of the personal data largely comply with the transparency requirements set out in Article 12(1) of the GDPR.

However, IMY finds that the description of the data contained in the technical log files provided by Spotify during the period from 11 June 2019 to 16 May 2022 has not complied with the requirements of Article 12(1) of the GDPR as this information has been provided by default only in English. Spotify has therefore processed personal data in this regard in breach of Article 12(1) of the GDPR during the period in question.

4 Review of individual complaints — Grounds for the decision

4.1 Complaint 1 (from the Netherlands with national reference number z2018-28415)

4.1.1 Background

In conclusion, the complainant submits that, with regards to his request of access made on 27 May 2018, Spotify AB has not granted access to all his personal data within the period laid down in Article 12(3) of the GDPR and that, once he has obtained access to all personal data, it has not been provided in an intelligible form as provided for in Article 12(1) of the GDPR.

¹⁶ Article 29 Working Party Guidelines on the right to data portability, WP242 rev.01, adopted by the European Data Protection Board, p. 19.

4.1.2 What Spotify AB has stated

Spotify AB provides three types of responses to ensure an appropriate and complete response to its users' requests under Article 15 of the GDPR. It states that information about all three types of responses (Type 1, Type 2 and Type 3) as well as information on how to request access to them was available at the time of the complainant's request. When a user chose to download their data (Type 1), the description and instructions given in connection with the download tool showed that this was only a convenient way to get a copy of "most" personal data from his or hers account and which categories of personal data were available through the tool. Based on the context, it was therefore sufficiently clear that other personal data were also available. The complainant also had the opportunity to contact customer service through a number of channels and request additional personal data. The complainant had also had the opportunity to turn to customer service and directly request access to all of his personal data.

Spotify AB considers that the process at that time was sufficiently transparent to allow users to understand and request additional available information in addition to those included in the tool "*Download Your Data*". Many other users also requested both Type 2 and Type 3 data at that time. The complainant also managed to request and access both Type 1 and Type 2 information. Spotify AB has since made several improvements in its processes to ensure that users cannot miss that there are three types of information and how to easily request access to that information.

Spotify AB states that, as regards the provision of the complainant's personal data, all requested personal data were provided within the timeframe set out in Article 12(3) of the GDPR. '*Download your data*' (Type 1) was requested by the complainant on 27 May 2018. The data were made available and downloaded by the complainant on 28 May 2018. A response time of one day is consistent with Spotify AB's goal of promptly providing the most relevant information to users through their automated tools.

Technical log files (Type 2) were requested by the complainant by email on 11 June 2018. In Spotify AB's reply on 6 July 2018, Spotify AB informed the complainant that the provision of personal data would take a little longer than expected due to the high number of requests and the complexity of compiling such technical information. The information was made available for download on 17 July 2018. Even after informing the complainant of the reason for the delay in replying, only 36 calendar days (26 working days) elapsed between the complainant's request and the receipt of a reply.

As regards the complainant's complaint concerning the format of the personal data, Spotify AB stated that Type 2 data contains a large number of files containing technical log data. The data processed may differ significantly for different users based on the type of Spotify service plan they have (e.g. Free, Premium, Family), features and the specific user's activity, as well as variations in the usual internal processing and error logging of Spotify AB's software itself. It is a challenge to find a way to explain this type of technical information in a way that the average Spotify user can understand.

At the time of the complainant's request, Spotify AB provided the information in a JSON format. However, it did not provide any additional documentation to further clarify the types of data included and how it should be interpreted (in addition to the information contained in the JSON data fields themselves). However, since 2019, Spotify AB provides an additional "Read Me First" file upon delivery of all Type 2 data, which further describes the information included in each file and data field. Given the complexity and volume of the technical log files, the preparation of the "Read Me First"

file required a lot of work, and Spotify AB had not yet completed this process at the time of the complainant's initial request of access.

It was a mistake that the complainant was provided with some of the technical log files in encrypted format. Spotify AB stores data in its systems in encrypted format in order to enhance the integrity and security of Spotify AB's own internal processing of personal data. It was not Spotify AB's intention to withhold the complainant's personal data from him. Although most encrypted data were decrypted before being included in the complainant's technical log files, some of the fields were not decrypted. This type of problem was addressed in the discovery of this, and now the requested personal data is always provided unencrypted.

Spotify AB would like to draw IMY's attention to the fact that the complainant requested his personal data again in July 2020. This request came after his complaint to IMY and the improvements described above. The complainant received his personal data much faster than within 30 days. The complainant requested "*Download your data*" (Type 1) on 28 July 2020. Spotify AB provided the personal data three calendar days later, on 31 July 2020. The complainant also requested its technical log files (Type 2) on 3 August 2020 and downloaded the personal data when available 15 days later, on 18 August 2020. Both of these requests were answered within a total of 18 days by Spotify AB and the complainant was able to receive all of its personal data within a total of 21 calendar days. This timeframe is representative of Spotify AB's handling of these types of requests from users. All the technical information received by the complainant on 18 August 2020 was unencrypted. The complainant should also have received a "Read Me First" file explaining the data provided in every field. With the fulfilment of the complainant's most recent request, Spotify AB hopes that all of the complainant's questions regarding Articles 12(1) and 12(3) of the GDPR that he raised in his complaint have been answered.

4.1.3 Assessment by the Swedish Authority for Privacy Protection

As IMY notes in the assessment of Spotify AB's general procedures, section 3.2.2 of this decision, it is possible to divide the copy of personal data into different layers provided that the data subject has received sufficient information on, among other things, how the copy of personal data is divided and how access to the different layers can be requested.

The complainant's claim that his personal data was not provided in due time shows that the complainant must have considered that his initial request sent on 27 May 2018 encompassed all the personal data Spotify AB processed about him. Furthermore, it is clear from the information provided by the complainant that he contacted Spotify AB because he himself noted that the copy of personal data he received on 28 May 2018 was not complete. The fact that he contacted Spotify AB was therefore a consequence of the conclusions made by the complainant himself on the basis of the copy of personal data he received and not because the complainant understood Spotify AB's way of dividing the copy of personal data and how access to additional information could be requested. In IMY's view, those circumstances imply that the information provided by Spotify AB at the time of the complainant's request concerning the way of dividing the copy of personal data was not sufficiently clear.

Furthermore, IMY considers, when assessing the information provided by Spotify AB in the description and instructions in connection with the complainant's Type 1 request on 27 May 2018, that that information itself was not sufficiently clear to the complainant so that he should have understood that only a subset of the personal data was covered

by the request. At the time of the complainant's request, the information currently available on Spotify AB's website, *inter alia*, on the "*personal data rights and privacy settings*" website, which lists the personal data provided in the various replies, and how access to these can be requested, was also missing. IMY also considers that Spotify AB's argument that the complainant could turn to customer service and request further information is irrelevant since such conduct presupposes that the complainant would have understood that there was additional personal data that could be provided.

In view of the above, IMY considers that, at the time of the complainant's request of access, Spotify AB did not provide sufficiently clear information to enable the complainant to understand that the copy of personal data was divided. The existence of sufficient information to enable a data subject to understand that his request relates only to a selection of the personal data being processed is a prerequisite for the controller to limit the disclosure to that personal data. Therefore, where it is unclear whether the request concerns only a selection of the personal data, the controller should assume that the data subject wishes to have access to all his or her personal data. Therefore, since the information in that regard was inadequate at the time of the complainant's request, Spotify AB should have provided all the personal data which they processed about the complainant at the time of his request of access made on 27 May 2018. The period within which Spotify AB had to provide the copy of all personal data shall therefore be calculated from that date. Pursuant to Article 12(3) of the GDPR, Spotify AB should have provided a full copy of the complainant's personal data or notified the complainant of an extension of the period by 27 June 2018. Spotify AB did not notify the complainant until 6 July 2018 of an extension of the period of time. The copy of the additional personal data was submitted on 17 July 2018. IMY notes that Spotify AB has not notified the extension within the time prescribed in Article 12(3) of the GDPR. Spotify AB has therefore provided the copy of the complainant's personal data too late.

The complainant's information, confirmed by Spotify AB, shows that the additional personal data he received on 17 July 2018 were difficult to understand and, in some cases, encrypted.

As IMY notes in section 3.2.2, the controller is required to explain personal data that is particularly difficult to understand in order to fulfil the purpose of the right of access. IMY notes that Spotify AB has not complied with its obligations in the complainant's case since it has not provided an explanation of the personal data particularly difficult to understand and since it has provided certain information encrypted.

In view of the above, IMY considers that in its handling of the complainant's request for access made on 27 May 2018, Spotify AB has processed personal data in breach of Article 12(3) of the GDPR, by not having provided the copy of personal data in due time, and in breach of Articles 12(1), 15(1) and 15(3) of the GDPR, by not having provided all of the complainant's personal data in an intelligible form.

4.2 Complaint 2 (from Austria with national reference number D130.198)

4.2.1 Background

The complainant submits that, with regard to his request for access made on 10 October 2018, Spotify AB has not provided all the personal data it processes about the complainant, that Spotify AB has not provided any of the information concerning the

processing of the complainant's personal data required by Article 15(1)(a) to (h) and (2) of the GDPR, and that Spotify AB has not provided the personal data in an intelligible form as provided for in Article 12(1) of the GDPR. In that regard, the complainant states, *inter alia*, that the data were provided in a format which is only machine-readable and not comprehensible to natural persons.

4.2.2 What Spotify AB has stated

Spotify AB stated that the complainant requested access to the '*Download Your Data*' (Type 1) on 10 October 2018. The data were made available and downloaded by the complainant on 18 October 2018. The complainant then never contacted Spotify AB again to present the views raised in his complaint to IMY. He also did not request access to additional personal data other than those made available through the '*Download Your Data*' tool.

Spotify AB provides three types of responses to ensure an appropriate and complete response to its users' requests under Article 15 of the GDPR. It states that information about all three types of responses (Type 1, Type 2 and Type 3), as well as information on how to request access to them, was available at the time of the complainant's request. When a user chose to download their data (Type 1), the description and instructions given in connection with the tool showed that this was only a convenient way to get a copy of "most" personal data from his or hers account and which categories of personal data were available through the tool. Based on the context, it was therefore sufficiently clear that other personal data were also available. The complainant also had the opportunity to contact customer service through a number of channels and request additional personal data.

Spotify AB considers that the process at that time was sufficiently transparent to allow users to understand and request additional available information in addition to those included in the tool "*Download Your Data*". Many other users also requested both Type 2 and Type 3 data at that time. Spotify AB has since made several improvements in its processes to ensure that users cannot miss that there are three types of information and how to easily request access to that information.

At the time of the complainant's request, the specific website with information pursuant to Article 15(1)(a) to (h) and (2) of the GDPR had not yet been created and such information was not automatically included in the response to the request for access. Spotify AB confirms that the complainant did not receive this information together with its Type 1 reply in October 2018. Spotify AB notes that although the complainant did not receive the specific information pursuant to Article 15 in connection with his request, the information was available to the complainant in Spotify AB's privacy policy.

Spotify AB further states that it had processes in place to provide additional information and to take action in the event that its response would not be considered sufficient to fully respond to a data subject's request of access. If the complainant had contacted privacy@spotify.com or Spotify AB's customer service team regarding his questions, they would happily provide additional personal data and other information pursuant to Article 15 of the GDPR that he requested.

It is true that the complainant's personal data provided through "*Download Your Data*" tool was provided in JSON format. JSON is a recommended standard format that can be understood by both people and computers. The information in "*Download Your Data*" (Type 1) is largely self-explanatory based on the name of the file and fields.

Nowadays, however, Spotify AB also provides a detailed description of the data on the information website "*Understand my data*".

4.2.3 Assessment by the Swedish Authority for Privacy Protection

As IMY notes in the assessment of Spotify AB's general procedures, section 3.2.2 of this decision, it is possible to divide the copy of personal data into different layers provided that the data subject has received sufficient information on, among other things, how the copy of personal data is divided and how access to the different layers can be requested.

The complainant, to IMY's understanding, wanted to have access to all the personal data Spotify AB processes about him. However, the complainant has only requested access to the Type 1 data and has not returned to Spotify AB for further information. In IMY's view, the complainant's conduct implies that the information provided by Spotify AB at the time of his request concerning the way of dividing the copy of personal data and how access to the various layers could be requested, was not sufficiently clear to enable him to understand how to obtain access to all the data.

Furthermore, IMY considers, when assessing the information provided by Spotify AB in the description and instructions in connection with the complainant's Type 1 request on 10 October 2018, that that information itself was not sufficiently clear to the complainant so that he should have understood that only a subset of the personal data was covered by the request. At the time of the complainant's request, the information currently available on Spotify AB's website, inter alia, on the "*personal data rights and privacy settings*" website, which lists the personal data provided in the various replies, and how access to these can be requested, was also missing. IMY also considers that Spotify AB's argument that the complainant could turn to customer service and request further information is irrelevant since such conduct presupposes that the complainant would have understood that there was additional personal data that could be provided.

In view of the above, IMY considers that, at the time of the complainant's request of access, Spotify AB did not provide sufficiently clear information to enable the complainant to understand that the copy of personal data was divided. The existence of sufficient information to enable a data subject to understand that his request relates only to a selection of the personal data being processed is a prerequisite for the controller to limit the disclosure to that personal data. Therefore, where it is unclear whether the request concerns only a selection of the personal data, the controller should assume that the data subject wishes to have access to all his or her personal data. Therefore, since the information in that regard was inadequate at the time of the complainant's request, Spotify AB should have provided all the personal data which they processed about the complainant. IMY notes that Spotify AB has not provided all the personal data they processed about the complainant. Spotify AB has therefore not complied with the requirements of Articles 15(1) and 15(3) of the GDPR to grant the data subject access to their personal data as Spotify AB has not provided the data subject with a complete copy of the personal data that was being processed.

The complainant further states that the personal data to which he has been given access were difficult to understand. It follows from Spotify AB's statement that, at the time of the complainant's request, there was no description of the personal data provided to the complainant (Type 1). However, IMY considers that the personal data provided according to a Type 1 request is sufficiently clear to enable the average user to understand the data and therefore does not require any further explanation. IMY

therefore considers that the personal data provided have been sufficiently clear to comply with the requirements of Article 12(1) GDPR, i.e. that the information provided under Article 15 of the GDPR should be provided in a concise, clear, intelligible and easily accessible form using clear and plain language. There was therefore no deficiency as to the clarity of the personal data provided to the complainant. However, IMY welcomes the improvements made by Spotify AB after this point, which may further increase the understanding of the personal data provided in Type 1 responses.

In addition, the complainant submits that his personal data were provided in a format which was only machine-readable and not comprehensible to natural persons. Spotify AB states that the data were provided in JSON format. IMY considers, as stated above under 3.2.2, that JSON format, which can be read by both computers and natural persons, is currently an electronic commonly used format as referred to in Article 15(3) of the GDPR. IMY therefore considers that there was no deficiency in the format in which the information was provided to the complainant.

Finally, the complainant claims that he did not receive information pursuant to Article 15(1)(a) to (h) and (2) of the GDPR. Spotify AB has confirmed that the complainant did not receive this information together with the reply to the request submitted in October 2018. Spotify AB has therefore failed to fulfil its obligation to provide information under Article 15(1)(a) to (h) and (2). The fact that at the time of the complainant's request information was available in Spotify AB's privacy policy does not affect this deficiency.

In conclusion, IMY considers that in its handling of the complainant's request for access made on 10 October 2018, Spotify AB has processed personal data in breach of Article 15(1) and (3) of the GDPR, by not having given access to all the personal data that Spotify AB processed about the complainant and in breach of Article 15(1)(a) to (h) and (2) of the GDPR, by not providing any of the information specified in these provisions.

4.3 Complaint 3 (from Denmark with national reference number 2018-31-1198)

The complainant claims that Spotify AB has not responded to the complainant's request of access under Article 15 of the GDPR made on 12 November 2018.

The investigation in the case has not shown that Spotify has failed in its handling of the complainant's request for access, with the result that the complaint in question should be rejected. The receiving supervisory authority, i.e. the Danish Data Protection Authority, is therefore to adopt the decision with regard to this complaint under Article 60(8) GDPR. The reasons for that decision is therefore set out in a separate decision adopted by the Danish Data Protection Authority.

5 Choice of corrective measure

5.1 Applicable provisions

In case of violations of the GDPR, IMY has a number of corrective powers, including reprimand, injunctions and administrative fines. This follows from Article 58(2)(a) to (j) of the GDPR.

IMY shall impose administrative fines in addition to or in place of other remedies referred to in Article 58(2) GDPR, depending on the circumstances of each case.

If a controller or processor, with respect to one or the same or linked data processing, intentionally or negligently violates several of the provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount determined for the most serious infringement. This is stated in Article 83.3 of the GDPR. Each supervisory authority shall ensure that the enforcement of administrative fines in each individual case is effective, proportional and deterrent. This is stated in Article 83(1) of the GDPR.

Article 83(2) states the factors to be taken into account in order to determine whether an administrative fine should be imposed, but also what should affect the size of the administrative fine.

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR, which aim to create a harmonised methodology and principles for the calculation of fines.¹⁷

5.2 Same or linked data processing

As stated above, IMY has, in the investigation carried out regarding Spotify AB's general processes and procedures for providing access pursuant to Article 15 of the GDPR, found deficiencies in the information provided pursuant to Article 15(1)(a) to (h) and (2) of the GDPR and in the description of the data in the technical log files provided by Spotify. Furthermore, Spotify AB has failed in its handling of requests for access relating to two of the complaints IMY has examined, complaint 1 and complaint 2.

The infringements related to the general procedures, relates, regarding the information provided under Articles 15(1)(a) to (h) and (2), to the period from 16 November 2021 to 16 May 2022 and, regarding the description of the data in the technical log files, to the period from 11 June 2019 to 16 May 2022. The requests for access covered by the individual complaints were made on 27 May 2018 and 10 October 2018 respectively. In this context, IMY assesses, inter alia, that the infringements related to the general procedures and the infringements relating to the two complaints do not constitute the same or linked processing operations within the meaning of Article 83(3) of the GDPR.

However, IMY considers that Spotify AB's provision of information covered by Article 15(1) and (2) of the GDPR and the provision of the description of the data in the technical log files is a linked processing. That assessment is made, inter alia, in the light of the fact that the deficiencies found in those parts relate to the transparency requirements of the information provided by Spotify to data subjects under Article 15 of

¹⁷ EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

the GDPR for a partially overlapping period of time. Furthermore, the complaints are deemed to be linked.

IMY should therefore separately determine the choice of corrective measure for the identified deficiencies in Spotify AB's general procedures, i.e. in the information pursuant to Article 15(1) and (2) of the GDPR and in the description of the data in the technical log files, and for the findings concerning the two complaints.

5.3 Infringements relating to the information pursuant to Article 15(1) and (2) GDPR and to the description of the data in the technical log files

IMY has considered that Spotify AB has infringed Articles 12(1), 15(1)(a) to (d), 15(1)(g) and 15(2) of the GDPR. Given, among other things, the fact that the infringements have been able to potentially affect a large number of data subjects, that the infringements have persisted over a long time and due to the fact that the deficiencies in the information has made it difficult for data subjects to exercise their other data protection rights, these are not minor infringements. Spotify AB should therefore be subject to an administrative fine in respect of the infringements in this part.

IMY notes that Spotify AB has infringed articles covered by Article 83(5) of the GDPR, which means that a fine of up to EUR 20 million or four per cent of the global annual turnover in the previous financial year, whichever is higher, can be imposed.

When determining the maximum amount for an administrative fine to be imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU (see recital 150 of the GDPR). The Court of Justice's case law states that this includes any entity engaged in economic activities, regardless of the unit's legal form and the way of its funding, and even if the unit in a legal sense consists of several natural or legal entities.

IMY considers that the company's turnover to be used as a basis for calculating the administrative fines that can be imposed on Spotify AB, is Spotify AB's parent company Spotify Technology S.A.'s. Spotify Technology S.A.'s annual report for 2021 shows that the annual turnover in 2021 was approximately SEK 132 000 000 000. The maximum administrative fine that can be determined in the case is 4 per cent of this amount, i.e. approximately SEK 5 280 000 000.

In assessing the seriousness of infringements, IMY takes into account, in addition to what is stated above, i.e. that the infringements have been able to potentially affect a large number of data subjects, that the infringements have persisted over a long time and that the deficiencies in the information have made it more difficult for data subjects to exercise their other data protection rights, the following. The infringements have led to a risk that the purpose of the right of access was undermined since the deficiencies in the information provided have made it difficult for data subjects to understand which of their personal data had been processed and how. The data subject has therefore not been able to check whether the processing has been lawful. Spotify AB's personal data processing also includes a large amount of personal data about each data subject and concerns many data subjects in several different countries.

However, as far as has been established, the data processed do not constitute special categories of personal data as set out in Article 9 of the GDPR. The processing of

personal data carried out in the context of a customer relationship when providing a music streaming service does not normally have significant consequences for the data subjects. Furthermore, despite the scope of Spotify AB's personal data processing, IMY has received only a few complaints regarding Spotify AB's handling of requests of access.

It is also of significance that Spotify AB has a challenge in providing comprehensive information about complex personal data processing in a way that is understandable to the data subjects, which entails a difficult balancing act when assessing how the information should best be presented. Spotify AB has provided some information in accordance with Article 15(1) and (2) of the GDPR. Furthermore, Spotify AB has provided information about its personal data processing on several pages on Spotify AB's website. Some information on how the personal data was processed has also been possible to extract from the copy of personal data pursuant to Article 15(3) of the GDPR that Spotify AB has provided to data subjects who requested access and which IMY has deemed to largely comply with the requirements for clarity in Article 12(1) of the GDPR.

The circumstances of the case further show that Spotify AB, on its own initiative and before the current supervisory case was initiated, has taken several measures and put extensive work on establishing, developing and improving procedures regarding requests of access in order to be transparent to the data subjects. These processes and procedures have since been continuously developed and improved. According to IMY, this indicates that Spotify AB intends to fulfil the right of access in a way that is transparent to the data subjects. Until last year, when the EDPB adopted guidelines on the right of access¹⁸, detailed guidance on how to provide the information and the level of detail, including the degree of individualization of the information to be provided under Article 15(1) and (2) of the GDPR as well as which language should be used when communicating under Article 15 GDPR, has also been missing.

Overall, considering the facts set out in this decision, IMY considers that the infringements in question are of a low degree of seriousness. The starting point for calculating the fine should therefore be set relatively low in relation to the maximum amount in question. In order to ensure a proportionate fine in the individual case, it is also necessary, at this stage, to further adjust the starting point for the further calculation downward, taking into account the high turnover underlying the calculation of the fine.

In addition to assessing the gravity of the infringement, IMY shall assess whether there are any aggravating or mitigating circumstances that have a bearing on the amount of the fine. The factors already taken into account in assessing the gravity of the infringement cannot be taken into account again at this stage of the assessment.

IMY considers that there are no further aggravating circumstances affecting the amount of the fine. As a mitigating circumstance, IMY places particular emphasis on the possibility for the data subjects to contact Spotify AB's customer service through several different channels to obtain additional personalised information. In addition, Spotify AB has informed in June 2022 that Spotify AB has made updates in the information pursuant to Article 15, among other things, to enable the data subject to understand the specific processing of personal data that is applicable to their unique use of Spotify AB Service. As regards the infringements relating to Spotify's choice of

¹⁸ European Data Protection Board (EDPB) Guidelines on the right of access — Guidelines 01/2022 on data subject rights — Right of access, (adopted on 18 January 2022 for public consultation and finally adopted on 28 March 2023).

language for the description of the data in the technical log files, it is also important that data subjects have had the opportunity to turn to Spotify to have the description translated or explained in their local language and that Spotify provided clear information about this possibility in the “Read Me First” file provided when the data was provided to the data subject.

Considering the seriousness, aggravating and mitigating circumstances of the infringements and the high turnover in relation to the infringements found, IMY determines the administrative fine for Spotify AB to SEK 58 000 000. IMY considers that this amount, which represents approximately 1 per cent of the maximum amount of the administrative fine that can be determined in the present case, is effective, proportionate and dissuasive in the present case.

5.4 Infringements relating to complaints 1 and 2

IMY has found that Spotify AB failed to fulfil its obligations vis-à-vis the complainants in complaints 1 and 2. However, IMY notes that, in both cases, the complainants have had access to some of their personal data in a timely manner. Furthermore, when the complainant in complaint 1 contacted them, Spotify AB has been helpful in providing further information and answering questions. Regarding complaint 2, Spotify AB has not been made aware that the complainant considered that his request of access had not been fully met. The complainant did not turn to Spotify AB to inform them that he was dissatisfied with Spotify AB’s handling of his request of access, hence Spotify AB had difficulties addressing the issue.

IMY notes that the current infringements did not involve sensitive personal data. In addition, Spotify AB adopted measures, albeit inadequate, in order to comply with the complainants’ requests. Therefore, even though the complainants’ right of access were not fully complied with, the deficiencies which existed are less serious than if the requests had been made unanswered.

IMY concludes from an overall assessment that, in relation to the infringements in complaints 1 and 2, there are minor infringements and that there is therefore reason to refrain from imposing a fine on Spotify AB for the infringements found in this part. Spotify AB shall instead be subject to a reprimand pursuant to Article 58(2)(b) of the GDPR.

Spotify AB states that it is willing to cooperate directly with the complainants in order to ensure that it has provided all the personal data and information wanted by the complainants and that it has answered their questions.

The complainant in complaint 1 reverted to Spotify AB in July 2020 and subsequently obtained access pursuant to Article 15 of the GDPR. The complainant received all of his personal data, including an explanatory document on the personal data processed, within 21 days. The personal data provided at the time was unencrypted. Since the complainant’s right of access has been satisfied, there is no reason to order Spotify AB to re-grant access in accordance with Article 15.

As regards complaint 2, there has been no information that the complainant has been given access to more personal data or more information following the response to the request of access in October 2018. Spotify AB should therefore, pursuant to Article 58(2)(c) of the GDPR, be ordered to comply with the complainant’s request of access under Article 15 of the GDPR by giving the complainant access to all personal data

that Spotify AB processes about him by providing him with a copy of the personal data pursuant to Article 15(3) of the GDPR and information pursuant to Article 15(1)(a) to (h) and (2) of the GDPR. In doing so, Spotify AB has to take into account the exceptions to the right of access in Article 15(4) of the GDPR and Chapter 5 of the Swedish Data Protection Act that may be applicable. Access should be provided within one month of the date of the entry into force of this Decision.

This decision was taken by [REDACTED] following a presentation by the legal advisors [REDACTED] and [REDACTED]. [REDACTED] also participated in the final proceedings.

Annex

Annex 1 — Complainant's identification data (complaint 2)

Annex 2 — Spotify AB's information pursuant to Article 15 GDPR, from 16 November to 16 May 2022.

Annex 3 — Information about payment of administrative fine

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision in case with national reference number, DI-2020-11370. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2020-11370

Date of decision:
2023-06-30

Final decision under the General Data Protection Regulation – Dagens Industri AB´s transfers of personal data to third countries

Table of contents

Decision of the Swedish Authority for Privacy Protection (IMY)	3
1 Presentation on the supervisory report.....	3
1.1 Processing	3
1.2 What is stated in the complaint	3
1.3 What Dagens Industri has stated	4
1.3.1 Who has implemented the Tool and for what purpose etc.	4
1.3.2 Recipients of the data.....	5
1.3.3 The data processed in the Tool and what constitutes personal data	5
1.3.4 Categories of persons concerned by the treatment	5
1.3.5 When the code for the Tool is executed and recipients are accessed	6
1.3.6 How long the personal data are stored	6
1.3.7 The countries in which personal data are processed	6
1.3.8 Dagens Industri´s relationship with Google LLC	6
1.3.9 Ensure that processing is not carried out for the purposes of the recipients	6
1.3.10 Description of Dagens industri´s use of the Tool.....	7
1.3.11 Own checks on transfers affected by the judgment in Schrems II	7
1.3.12 Transfer tools under Chapter V of the GDPR.....	8
1.3.13 Verification of obstacles to compliance in third country legislation	8
1.3.14 Supplementary measures taken in addition to those taken by Google	8

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

1.3.15 Dagens industri's assessment and conclusion regarding whether the data can be considered identifiable.....	11
1.4 What Google LLC has stated	13
2 Statement of reasons for the decision	14
2.1 The framework for the audit	14
2.2 This is the processing of personal data.....	14
2.2.1 Applicable provisions, etc.....	14
2.3 Dagens Industri is the data controller for the processing.....	17
2.4 Transfer of personal data to third countries	18
2.4.1 Applicable provisions, etc.....	18
2.4.2 Assessment by the Swedish Authority for Privacy Protection (IMY)	20
3 Choice of intervention	23
3.1 Applicable provisions	23
3.2 Should an administrative fine be imposed?	24
3.3 Other interventions.....	25
4 How to appeal.....	26

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority Authority for Privacy Protection finds that the investigation has shown that Dagens Industri Aktiebolag processes personal data in breach of Article 44 of the GDPR¹ by using the Google Analytics tool provided by Google LLC on its website www.di.se, and thereby transferring personal data to third countries without the conditions laid down in Chapter V of the Regulation being met, since 14 August 2020 and until the date of this decision.

Pursuant to Article 58(2)(d) of the GDPR, the Dagens Industri Aktiebolag is required to ensure that the company's processing of personal data in the context of the company's use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, Dagens Industri Aktiebolag shall cease to use the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards have been taken. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

1 Presentation on the supervisory report

1.1 Processing

The Swedish Integrity Authority for Protection Authority (IMY) has initiated supervision regarding Dagens Industri AB (hereinafter Dagens Industri or the company) due to a complaint. The complaint has claimed a breach of the provisions of Chapter V of the GDPR related to the transfer of the complainant's personal data to third countries. The transfer is alleged to have taken place when the complainant visited the company's website, www.di.se (hereinafter "the company's website" or the "Website") through the Google Analytics tool (hereinafter the Tool) provided by Google LLC.

The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Austria) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned has been the data protection authorities in Germany, Norway, Denmark, Estonia and Portugal.

1.2 What is stated in the complaint

The complainant essentially stated the following.

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).

On 14 August 2020, the complainant visited Dagens Industri's website. The complainant visited the controller's website, while being logged in to the Google/Facebook account associated with the complainant's email address. On the website, the controller has embedded a JavaScript code for Google/Facebook services including "Google Analytics" or "Facebook Connect". In accordance with paragraph 5.1.1(b) of the terms and conditions of Google's processing of personal data for Google's advertising products and also Google's terms and conditions for processing the New Google Ads Processing Terms, for Google Advertising Products, Google processes personal data on behalf of the controller (i.e. Dagens Industri) and is therefore to be classified as the company's data processor.

During the visit to the company's website, Dagens Industri processed the complainant's personal data, at least the complainant's IP address and the data collected through cookies. Some of the data has been transferred to Google. In accordance with Section 10 of the Terms and Conditions on the Processing of Personal Data for Google's Advertising Products, Dagens Industri has authorised Google to process personal data of the Applicant in the United States. Such transfer of data requires legal support in accordance with Chapter V of the GDPR.

According to the judgment of the Court of Justice of the European Union (CJEU), in Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II), the company² could no longer rely on an adequacy decision under Article 45 of the GDPR for the transfer of data to the United States. Dagens Industri should not base the transfer of data on standard data protection clauses under Article 46(2)(c) GDPR if the recipient of the personal data in third country does not ensure appropriate protection with regard to Union law for the personal data transferred.

Google shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881 (4)(b) and is thus subject to surveillance by U.S. intelligence services in accordance with 50 US § 1881a (Section 702 of the Foreign Intelligence Surveillance Act, below "702 FISA").³ Google provides the U.S. government with personal data in accordance with these provisions. Dagens Industri cannot therefore ensure adequate protection of the complainant's personal data when it is transmitted to Google.

1.3 What Dagens Industri has stated

Dagens Industri Aktiebolag has essentially stated the following.

1.3.1 Who has implemented the Tool and for what purpose etc.

The code for the Tool was embedded on the Website at the time of the complaint and is still embedded on the Website. The decision to embed the Tool on the Website was made by Dagens Industri, a company registered in Sweden. Data is collected from all persons visiting the Website, which is likely to include data subjects from more than one EU/EEA Member State.

² Judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

³ See <https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm> and <https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881a.htm>.

The purpose of embedding the code for the Tool on the Website is to enable Dagens Industri to analyse how the Website is used, in particular to be able to monitor the use of the Website over time.

The Website is aimed at Swedish visitors, but it cannot be excluded that individuals from other countries have visited the Website and thus may be included in the statistics.

The data (including any personal data) transmitted to the Tool may be stored on servers in different countries, including the United States. As a user of the Tool, it is not possible to control which servers are used to store data in the Tool.

1.3.2 Recipients of the data

In the context of Dagens Industri's use of the Tool on the Website, personal data is disclosed to a number of actors, all of which are data processors or sub-processors to Dagens Industri, including Google LLC, Google Ireland Ltd and their sub-processors.

1.3.3 The data processed in the Tool and what constitutes personal data

Within the framework of Dagens Industri's use of the Tool on the Website, the company and its personal data processors (the recipients) process the following data.

- *Page view data* — such as URL, clicks in menus, articles visited, reading time, and how long the visitor is watching a video.
- *Device technical information* — such as cookie value (which is hashed before it is transferred to the Tool, but was not hashed when the complainant visited the Website), operating system and screen size.
- *User category* — for example, a flag that shows whether the visitor is a subscriber or not.⁴
- *So-called "own dimensions"* — for example, which version of the publishing platform on which a page view took place, information about article (e.g. author).
- *IP Addresses* — The IP address is processed both when Google Analytics *is measured script and when measured data are to be transferred* to the Tool. The IP address processed together with measured data (page view data, etc.) is anonymised through the company's proprietary process and which is handled on an EU-based infrastructure before it is sent together with the measured data to the Tool (see more about this below).

Dagens Industri considers that the *categories* page view data, technical information about device, user category and “own dimensions” can be considered personal data only in cases where the company can link this data to an individual through additional information that the company has in other systems, which is not always the case. Dagens Industri considers IP addresses as personal data until these are anonymised.

1.3.4 Categories of persons concerned by the treatment

The *categories* of persons concerned by the processing are visitors to the Website. It can be Dagens Industri's paying subscribers or visitors without a digital account.

⁴ Please note that identifying information such as actual subscription ID is not transferred, but only a value representing the category “subscriber” or “not subscriber” (1 or 0).

Data on particularly vulnerable persons are not processed. The Website is primarily aimed at adults in their professional role or who have an interest in economics and nutrition issues. It is not aimed at children or other particularly vulnerable groups.

1.3.5 When the code for the Tool is executed and recipients are accessed

The code for the content of the Tool, i.e. the script that measures the data sent to the Tool, is only executed if the visitor has given their consent to Dagens Industri using analytics cookies on the Website. If the visitor has given their consent, the data measured by the script will first be sent to Dagens Industri's proxy server, where several security-enhancing measures are implemented, such as anonymisation of IP address. A subset of the measured data is then transferred encrypted from the proxy server to the tool provided by Google (see below).

Google LLC, Google Ireland and other data processors and subprocessors have access to the pseudonymised data stored in the Tool to the extent necessary for the processor or subprocessor to perform the service, including support and troubleshooting services.

1.3.6 How long the personal data are stored

The data measured on the Website and transmitted to the Tool will be stored in the Tool for 26 months and then deleted. Dagens Industri saves the data in order to analyse the use of the Website over time, in order to be able to make annual comparisons and thereby analyse how the usage changes. Dagens Industri has considered that it is necessary to at least be able to compare the use over two years cycles. In order to analyse and produce statistics on these changes, the company needs to save the measured data for 26 months.

1.3.7 The countries in which personal data are processed

The data transmitted to the Tool is stored in, for example, the United States.

1.3.8 Dagens Industri's relationship with Google LLC

The Tool is provided by agreement between Dagens Industri and a Swedish limited company (hereinafter the "Supplier"). Google Ireland Ltd is in turn a subcontractor to the supplier. Dagens Industri has entered into a personal data processor agreement with the supplier, which regulates the supplier's and its sub-processes' personal data processing.

Since the purposes and means of the processing as a whole are determined by Dagens Industri, Google LLC and Google Ireland Ltd are processors for the personal data processing that becomes relevant in relation to the Tool.

Dagens Industri has also entered into a data processing agreement directly with Google LLC to comply with the formal requirements of the standard contractual clauses, i.e. that these be formally entered into directly between the controller and the third country processor.

1.3.9 Ensure that processing is not carried out for the purposes of the recipients

1.3.9.1 Generally

Dagens Industri cares to use only suppliers that can meet the company's high requirements for safe and lawful personal data processing. Before selecting a particular supplier, an assessment is made of the supplier's ability to maintain an acceptable level of security, including protecting personal data to be processed.

Dagens Industri has also developed an audit plan in which the company intends to carry out audits of the most important suppliers, based on a rolling schedule. Dagens Industri has also engaged in a continuous dialogue with Google, where security and data protection issues are discussed.

1.3.9.2 Contracts with the Supplier

Through the assistance agreement with the supplier and the documented instructions given by Dagens Industri in this respect, it has been contractually ensured that the supplier and its sub-processors do not process personal data for their own or third parties' purposes. The Assistance Agreement thus contains special provisions (section 3.2.1) that the supplier may only process personal data in accordance with Dagens Industri's documented instructions. Annex 2 to the Processing Agreement clarifies that the supplier under no circumstances has the right to process personal data for his own purposes.

As an incentive to comply with the requirements set out in the assistance agreement and to point out its weight, the Supplier has a liability to Dagens Industri if the Supplier should violate the agreement or applicable data protection legislation and this causes damage to Dagens Industri.

The assistance agreement with the supplier also enables Dagens Industri to request documentation and carry out audits of systems and procedures to ensure that the processing is carried out in accordance with Dagens Industri's documented instructions and applicable data protection legislation.

If Dagens Industri has reason to believe that the supplier does not comply with the requirements set out in the assistance agreement, Dagens Industri intends to conduct such an audit. The Provider also has the right to request documentation and to conduct audits in relation to Google (Section 7.5 of Google's Agreement).

Dagens Industri may also request to conduct audits of Google's systems and procedures in accordance with the Assistant Agreement with the Supplier (Section 8.5).

1.3.10 Description of Dagens industri's use of the Tool

Dagens Industri uses the Tool to collect quantitative data, web statistics, how the Website is used, and perform analyses based on this data. For example, web statistics can show which pages are most visited, which route visitors take through the Website, and from which pages visitors leave the Website. Web analytics can also provide insight into the frequency of visits and what content is visited for the longest time. For example, the analysis carried out using the Tool can serve as the basis for product improvements.

1.3.11 Own checks on transfers affected by the judgment in Schrems II

Following the publication of the Schrems II judgment on 16 July 2020, Dagens Industri launched a project to generally map transfers of personal data to third countries at the end of July 2020. The project did not specifically address the tool, but concerned third country transfers in general. In connection with Dagens Industri's becoming aware of, inter alia, the complaint at issue, a project specifically related to the use of the Tool was initiated on 18 August 2020. Relatively immediately after the judgment, the company was able to conclude that it is relevant to the data transmission that takes place within the framework of the Tool and Dagens Industri has subsequently implemented relevant safeguards, see below.

1.3.12 Transfer tools under Chapter V of the GDPR

Dagens Industri has entered into a personal data processing agreement directly with Google LLC. Google's standard contractual clauses are part of the assistance agreement. The assistant agreement states that Google is bound by the clauses (paragraph 10.2). The clauses are based on Commission Decision 2010/87/EU for transfers from a controller within the EU/EEA to a processor outside the EU/EEA. These terms and conditions apply automatically upon the conclusion of Google's Data Processing Agreement and thus do not need to be signed separately in order to be applicable. This is apparent from the preamble to Google's standard contractual clauses. Under Swedish law, which applies to the standard contractual clauses, this means that they become part of the contract.

Google's standard contractual clauses are also part of the Data Processing Agreement with the supplier in accordance with Annex 2 of the Processing Agreement with the supplier.

Dagens Industri has also entered into a data processor agreement with the supplier, in which Google Ireland Ltd acts as subprocessor and which in turn has some sub-processors in third countries. For the purposes of this Agreement, Google's standard contractual clauses are also applied as a transfer tool.

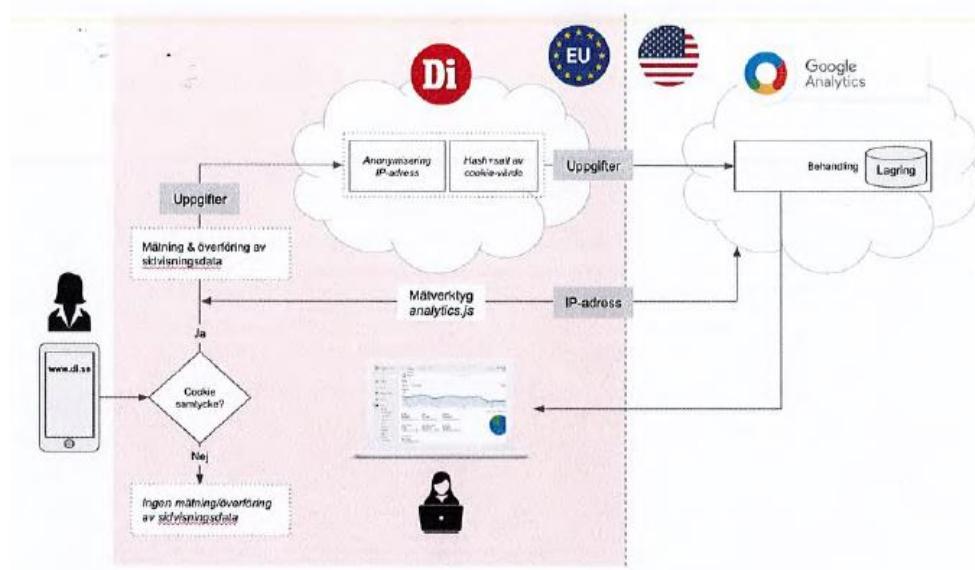
1.3.13 Verification of obstacles to compliance in third country legislation

Dagens Industri has not yet been able to establish with certainty whether there is anything in third country legislation that prohibits beneficiaries from fulfilling their contractual obligations under the standard contractual clauses. The company has therefore presumed that this is the case and has put in place specific technical measures to ensure that the protection of the data processed in the Tool reaches an acceptable level.

1.3.14 Supplementary measures taken in addition to those taken by Google

1.3.14.1 Introduction

Dagens Industri has carried out a comprehensive mapping of the life cycle of personal data processed in the Tool, identifying and implementing a number of supplementary measures. The measures are visualised at a glance in the picture below, and are further commented in the following sections.



1.3.14.2 Control of the collection and transmission of data to the Tool

A common way of using the Tool, unless supplementary measures are taken, means that the data measured through the Website's measuring script is transferred directly to the servers of the Tool, without first going through a control point of the controller using the tool.

Because the Tool's servers may be located inside and outside the EU/EEA, the use of the tool may lead to the transfer of measured data to third countries. The Tool has a function that allows users of the tool to choose to anonymise the IP address (truncating)⁵ that is transmitted together with the measured data. Since anonymisation occurs only after the IP address is transferred to Google Analytics servers, according to Dagens Industri, a third country transfer occurs before anonymisation takes place.

Dagens Industri has taken supplementary measures before data is transferred to the Tool. In order to take control of what data is transferred to the servers of the Tool outside the EU/EEA, the Company has implemented technical measures whereby the data collected through Google Analytics measurement script on the Website are transferred in a first step to a proxy server located in the EU where the data are processed in order to avoid that they can be used to identify an individual accordingly. The software used has been developed and owned by Dagens Industri, and is hosted by Google Ireland Ltd as part of the Google Cloud Platform ("GCP"). The GCP is thus used only as leased infrastructure to run the proxy server code on. The data processed on the GCP takes place exclusively at data centres in the EU. Dagens Industri is responsible for the personal data that takes place in the proxy server.

By introducing this control point, Dagens Industri can ensure that no data is transferred to servers outside the EU/EEA without having first undergone protective measures (see further below). Transmission to the proxy server is encrypted using Secure Sockets Layer ("SSL"), a technology that is encrypted communication between a web-server and a server).

⁵ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

1.3.14.3 Anonymisation of IP address and algorithm

The data that in some cases can be linked to an individual and transferred from the Website to the proxy server is the IP address and cookie value. The examples below illustrate how these numbers can look before and after they are processed on the proxyserver.

Before processing on proxy server:

Data

- IP address: clear text, e.g. 176.10.253.34
- Cookie value: clear text, e.g. 744100309.1604572939

Before transferring the measured data to the Tool, the following is performed on the proxy server:

- *Anonymisation of IP address.* The visitor's IP address is anonymised by generalisation and aggregation where the last octet of the IPv4 address is replaced by ".0".
- *Hashing of the cookie value.* The cookie value measured on the Website can either be completely anonymous (when the company *cannot* link the cookie value to data in its other systems) or constitute a pseudonymised personal data (when the company can link the cookie value to data in its other systems). As a supplementary measure before transferring to the tool, the cookie value from the visitor's client with a "salt" has been collected.⁶ The hashing of the cookie value further protects against the risk that U.S. authorities may link "intercepted data" (i.e. data that could possibly be read through signals intelligence programs either "at rest" in the Tool or "in transfer") with identifying data to which U.S. authorities might otherwise be able to access.

If the actions described above have been carried out, the IP address and the cookie value may, for example, look as follows:

Data

- IP address: anonymised, e.g. 176.10.253.00
- Cookie value: hashad, e.g. 35009a79-1a05-49d7-b876-2b884d0f825b

The data is then transferred via SSL encryption from the proxy server to the Tool.

Anonymisation of the visitor's IP address takes place when it is to be transmitted together with the measured page view data, etc. (see above for which data points are measured).

Prior to that, the IP address was exposed to the Tool when Google Analytics measured script via encrypted transmission was loaded into the visitor's browser from the Tool's server. It is not possible to link the IP address to the page view data etc. which is later measured on the Website. Dagens Industri has therefore assessed that

⁶ Cf. information on "Keyed-hash function with stored key" in the Article 29 Working Party's guidance on anonymisation techniques.

this exposure to the IP address does not pose a risk of privacy for visitors to the Website.

Google LLC may indirectly derive the time of the visit, but this possibility is very limited. Google has configured the server whereupon ‘analytics.js’ is provided in such a way that the JavaScript file is cached in the application cache of the receiving terminal for two hours, regardless of which website it is first obtained through (i.e. not necessarily on the Website). During this time period, no further calls are made in which the IP address is exposed in its entirety, which means that the measured page view data transmitted via Dagens Industri’s proxy server to Google LLC (first transmission) very rarely have a corresponding time equivalent machine log of Google LLC linked to the transmission via “analytics.js” (second transmission). In combination with the fact that visitors most often use the Website as a source of information in the work and/or during the previous two hours visited another website that uses Google Analytics (maximum likely given that about 74 % of the world’s 10,000 most popular websites present) a large percentage of visits to the Website only result in transmitted page view data from Dagens Industri’s proxy server and no loading of the Tool and associated transmission of IP address. This greatly complicates any attempt to link machine logs from the transfer of the Tool and transmitted page view data from Dagens Industri’s proxy server and reduces according to Dagens Industri risk to beyond “reasonable probability”.

1.3.14.4 More on checking that further measures can be implemented in practice, etc.
Dagens Industri considerations regarding the measures implemented by the company are based on the EDPB’s recommendations on how individual third country transfers should be assessed according to their specific legal context (paragraph 33).⁷

The security-enhancing measures consist primarily of the responsibility and control that Dagens Industri has taken over the phases of the life cycle before transferring the data to the Tool. The risk assessment has had as a starting point that the data subject’s protection is best achieved by the fact that the data transferred outside the EU/EEA are disconnected from the data subject and his/her technical unit used to visit the Website, and that the Company controls the process that ensures that these actions are carried out.

1.3.14.5 Dagens Industri’s conclusion on an adequate level of safety protection
Taking into account the measures implemented, Dagens Industri considers that the risk that the data subjects’ privacy or rights would be violated by the use of the Tool is very small. The company’s overall assessment is therefore that an adequate level of protection is achieved through the supplementary measures implemented.

1.3.15 Dagens industri´s assessment and conclusion regarding whether the data can be considered identifiable

1.3.15.1 The Company’s assessment of whether the data can be considered identifiable

Dagens Industri believes that it is not self-evident that an assessment leads to the data in question — IP address, certain system information and visited URL — constitute personal data.

⁷ EDPB Recommendation 01/2020 on measures to complement transfer tools to ensure compliance with the EU level of personal data protection Version 2.0 Adopted on 18 June 2021

Recital 26 of the GDPR states, *inter alia*:

'In order to determine whether a natural person is identifiable, account should be taken of all means, such as excavation, which, either by the controller or by another person, may reasonably be used to identify the natural person directly or indirectly. In order to determine whether means are reasonably likely to identify the natural person, account should be taken of all objective factors, such as the costs and time needed for identification, taking into account the technology available at the time of processing as technological progress.'

In its guidance on the concept of personal data,⁸ the Article 29 Working Party has further clarified how the assessment should be carried out:

Recital 26 to Directive 95/46⁹ (repealed) *pays particular attention to the term "identifiable"* when it reads that "whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person." This means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". If, taking into account "all the means likely reasonably to be used by the controller or any other person", that possibility does not exist or is negligible, the person should not be considered as "identifiable", and the information would not be considered as "personal data". The criterion of "all the means likely reasonably to be used either by the controller or by any other person" should in particular take into account all the factors at stake. The cost of conducting identification is one factor, but not the only one. The intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures should all be taken into account.¹⁰

In addition, the guidance states:

*"One relevant factor, as mentioned before, for assessing "all the means likely reasonably to be used" to identify the persons will in fact be the purpose pursued by the data controller in the data processing."*¹¹

1.3.15.2 Dagens Industri's conclusion as to whether the data can be considered identifiable

Dagens Industri has concluded that in order for it to be personal data according to the GDPR, the assessment of whether individuals are identifiable should be based on all relevant circumstances and assess the reasonable likelihood of identification, of which the purpose of the processing is a circumstance. Since the purpose of the processing is not to identify individuals, technical protection measures are an extra important factor in assessing whether individuals may be identified.

Against this background, Dagens Industri concludes that it is not self-evident that an assessment in accordance with the Article 29 Working Party's guidance means that the data in question — IP address, certain system information and web address visited

⁸ WP 136. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007

⁹ 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.

¹⁰ WP 136. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007, page 15.

¹¹ WP 136. Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007, pages 16 and 17.

— constitute personal data.

The assessment that individuals are not identifiable has been made taking into account the circumstances shown in i.e. (i) the cost of identification, (ii) the purpose of the processing, (iii) the structure of the processing, (iv) the benefits that the controller expects from the processing, (v) the interests at stake for the natural person, and (vi) the duration of the processing. The purpose of the processing is not to identify individuals but constitute technical protection measures. According to Dagens Industri, it is not at all obvious that an assessment in accordance with the guidance leads to the data in question — IP address, certain system information and visited URL — constitute personal data.

1.4 What Google LLC has stated

IMY has added to the case an opinion of Google LLC (Google) on 9 April 2021 submitted by Google to the data protection authority in Austria. The opinion answers questions asked by IMY and a number of regulators to Google in response to partial joint handling of similar complaints received by these authorities. Dagens Industri has been given the opportunity to comment on Google's opinion. Google's opinion shows the following about the Tool.

A JavaScript code is included on a web page. When a user visits (calls) a web page, the code triggers a download of a JavaScript file. After that, the Tool tracking operation, which consists of collecting information related to the call in different ways and sending the information to the server of the Tool, is performed.

A website manager who integrated the Tool on his website may send instructions to Google for the processing of the data collected. These instructions are transmitted via the so-called tag manager who manages the tracking code that the webmaster has integrated into his website and through the tag manager's settings. The person who integrated the tool can make different settings, for example regarding storage time. The Tool also enables those who integrated it to monitor and maintain the stability of their website, for example by keeping themselves informed of events such as peaks in visitor traffic or lack of traffic. The Tool also enables a website manager to measure and optimize the effectiveness of advertising campaigns carried out using other Google tools.

In this context, the Tool collects visitor's http calls and information about, among other things, the visitor's browser and operating system. According to Google, a http call for any page contains information about the browser and device making the call, such as domain names, and information about the browser, such as type, reference and language. The Tool stores and reads cookies in the visitor's browser to evaluate the visitor's session and other information about the call. Through these cookies, the Tool enables unique users (UUID) identification over browsing sessions, but the Tool cannot identify unique users in different browsers or devices. If a site owner's website has its own authentication system, the site owner can use the ID feature to identify a user more accurately on all the devices and browsers they use to access the site. When the information is collected, it is transferred to the servers of the Tool. All data collected through the Tool is stored in the United States.

Google has put in place, among other things, the following legal, organisational and technical measures to regulate transfers of data within the framework of the Tool.

Google has put in place legal and organisational measures, such as that it always conducts a thorough review of a request for access from government authorities if user data can be implemented. It is lawyers/specially trained staff who conduct these trials and investigate whether such a request is compatible with applicable laws and Google's guidelines. Data subjects are informed of the disclosure, unless prohibited by law or would adversely affect an emergency. Google has also published a policy on its website on how to implement such a request for access by government authorities of user data.

Google has put in place technical measures such as protecting personal data from interception when transmitting data in the Tool. By default, using HTTP Strict Transport Security (HSTS), which instructs browsers such as http to SSL (HTTPS) to use an encryption protocol for all communication between end-users, websites, and tool servers. Such encryption prevents intruders from passively listening by communications between websites and users.

Google also uses encryption technology to protect personal data known as "data at rest" in data centers, where user data is stored on a disk or backup media to prevent unauthorised access to the data.

In addition to the above actions, website owners may use IP anonymisation by using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated and contribute to data minimisation. If the IP anonymisation service is fully used, the anonymisation of the IP address takes place almost immediately after the request has been received.

Google also restricts access to the data from the Tool through permission control and by all personnel having completed information security training.

2 Statement of reasons for the decision

2.1 The framework for the audit

Based on the complaint in the case, IMY has only examined whether Dagens Industri transfers personal data to the third country USA within the framework of the Tool and whether the company has legal support for it in Chapter V of the GDPR. Supervision does not apply if the Dagens Industri's personal data processing is otherwise in accordance with the GDPR.

2.2 This is the processing of personal data

2.2.1 Applicable provisions, etc.

In order to determine whether the data processed through the Tool constitute personal data, IMY shall decide whether Google or Dagens Industri, through the implementation of the Tool, can identify individuals, e.g. the complainant, when visiting the Website or whether the risk is negligible.¹²

¹² See the Administrative Court of Appeal in Gothenburg's judgment of 11 November 2021 in case No 2232-21, with the agreement of the lower court.

IMY considers that the data processed constitute personal data for the following reasons.

The investigation shows that Dagens Industri implemented the Tool by inserting a JavaScript code (a tag), as specified by Google, into the source code of the Website. While the page loads in the visitor's browser, the JavaScript code is loaded from Google LLC's servers and runs locally in the visitor's browser. A cookie is set simultaneously in the visitor's browser and stored on the computer. The cookie contains a text file that collects information about the visitor's operation on the Website. Among other things, a unique identifier's set in the value of the cookie and this unique identifier is generated and managed by Google.

When the complainant visited the Website, or a subpage of the Website, the following information was transmitted via the JavaScript code from the complainant's browser to Google LLC's servers:

1. Unique identifier(s) that identified the browser or device used to visit the Website and a unique identifier that identified Dagens Industri (i.e. the Dagens Industri account ID for Google Analytics).
2. URL and HTML title of the website and web page visited by the complainant;
3. Information about browser, operating system, screen resolution, language setting, and date and time of access to the Website.
4. The complainant's IP address.

At the time of the complainant's visit, the identifiers referred to in paragraph 1 above were set in cookies with the names '_gads', '_ga' and '_gid' and subsequently transferred to Google LLC. Those identifiers were created with the aim of distinguishing individual visitors, such as the complainant. The unique identifiers thus make visitors to the Website identifiable. However, even if such unique identifiers (according to 1 above) were not in themselves to make individual identifiable, it must be borne in mind that, in the present case, those unique identifiers may be combined with additional elements (according to paragraphs 2 to 4 above) and that it is possible to draw conclusions in relation to information (as set out in paragraphs 2 to 4 above) from which data constitute personal data, irrespective of whether the IP address was not transmitted in its entirety.

Combined data (according to points 1-4 above) means that individual visitors to the Website become even more separable. It is therefore possible to identify individual visitors to the Website. This in itself is sufficient for it to be considered personal data. Knowledge of the actual visitor's name or physical addresses is not required, as the distinction (by the word 'release' in recital 26 of the GDPR, 'singling out' in the English version) is sufficient in itself to make the visitor indirectly identifiable. Nor is it necessary for Google or Dagens Industri to identify the complainant, but the possibility of doing so is in itself sufficient to determine whether it is possible to identify a visitor. *Objective means that can reasonably be used* either by the controller or by another, are *all means that can reasonably be used* for the purpose of identifying the complainant. Examples of *objective means that can reasonably be used* are access to additional information from a third party that would allow the complainant to be identified taking into account both the available technology at the time of identification and the cost (time required) of the identification.

IMY notes that, in its judgments in M.I.C.M. and Breyer, the Court of Justice of the European Union held that dynamic IP addresses constitute personal data in relation to

the person processing them, where it also has a legal means to identify the holders of internet connections using the additional information available to third parties.¹³ IP addresses do not lose their character of being personal data simply because the means of identification lie with third parties. The Breyer judgment and the M.I.C.M judgment should be interpreted on the basis of what is actually stated in the judgments, i.e. if there is a lawful possibility of access to additional information for the purpose of identifying the complainant, it is objectively clear that there is a '*legal means which enable it*' to identify the complainant. According to IMY, the judges should not be read in contrast, in such a way as to demonstrate a legally regulated possibility of access to data that could link IP addresses to natural persons in order for the IP addresses to be considered personal data. In IMY's view, an interpretation of the concept of personal data which implies that there must always be a *legal possibility* of linking such data to a natural person would constitute a significant restriction on the area of protection of the Regulation and would open up the possibility of circumventing the protection provided for in the Regulation. That interpretation would, *inter alia*, run counter to the objective of the Regulation as set out in Article 1(2) of the GDPR. The Breyer judgment is decided under Directive 95/46 previously in force and the notion of 'singling out' as set out in recital 26 of the current regulation (not requiring knowledge of the actual visitor's name or physical address, since the distinction itself is sufficient to make the visitor identifiable), was not mentioned in the previous directives as a means of identifying personal data.

In this context, there are also other data (according to paragraphs 1 to 3 above) with which the IP address can be combined to enable identification. Google's action regarding¹⁴ the truncation of an IP address means that the IP address can still be distinguished as it can be linked to other data transmitted to third countries (to the United States). This enables identification, which in itself is sufficient for the data to constitute personal data together.

In addition, several other supervisory authorities in the EU/EEA have decided that the transfer of personal data to third countries has taken place in the use of the Tool because it has been possible to combine IP addresses with other data (according to paragraphs 1 to 3 above), thus enabling the separation of data and the identification of the IP address, which in itself is sufficient to determine the processing of personal data.¹⁵

IMY notes that there may also be reasons to compare IP addresses with pseudonymised personal data. In accordance with Article 4(5) of the GDPR, pseudonymisation of personal data means that the data — like dynamic IP addresses — can no longer be attributed to a specific data subject without the use of additional information. According to recital 26 of the GDPR, such data should be considered to be data relating to an identifiable natural person.

¹³ Judgment of the Court of Justice of the European Union M.I.C.M, C-597/19, EU:2021:492, para. 102-104 and Breyer, C-582/14 EU:C:2016:779, paragraph 49.

¹⁴ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this action means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.

¹⁵ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

According to IMY, a narrower interpretation of the concept of personal data would undermine the scope of the right to the protection of personal data, as guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, as it would allow controllers to specifically designate individuals together with personal data (e.g. when they visit a particular website) while denying individuals the right to protection against the dissemination of such data. Such an interpretation would undermine the level of protection of individuals and would not be compatible with the broad scope of the data protection rules laid down in the case-law of the Court of Justice of the European Union.¹⁶

Furthermore, Dagens Industri, by being logged in to its Google account when visiting the Website, processed data from which it was able to draw conclusions about the individual on the basis of his registration with Google. Google's opinion shows that the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a data subject) has visited the website in question. It is true that Google states that certain conditions must be met in order for Google to receive such information, such as that the user (applicant) has not disabled the processing and display of personal ads. Since the applicant was logged in to its Google account when visiting the Website, Google may still have been able to obtain information about the logged-in user's visit to the Website. The fact that it is not apparent from the complaint that no personalised ads have been displayed does not mean that Google cannot obtain information about the logged-in user's visit to the Website.

In the light of the unique identifiers capability of identifying the browser or device, the ability to derive the individual through its Google account, the dynamic IP addresses and the possibility of combining these with additional data, Dagens Industri's use of the Tool on a website, means the processing of personal data.

2.3 Dagens Industri is the data controller for the processing

The controller is, among other things, the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4(7) GDPR). The processor is, among other things, a legal person who processes personal data on behalf of the controller (Article 4(8) GDPR).

The responses provided by Dagens Industri indicate that the company has made the decision to implement the Tool on the Website. It also appears that Dagens Industri's purpose was to enable the company to analyse how the Website is used, in particular to be able to monitor the use of the website over time.

IMY finds that Dagens Industri, by deciding to implement the Tool on the Website for that purpose, has determined the purposes and means of the collection and subsequent transfer of this personal data. Dagens Industri is therefore the data controller for this processing.

¹⁶ See, for example, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:2021:504, paragraph 61; Nowak, C-434/16, EU:2017:994, paragraph 33; and Rijkeboer, C-553/07, EU:2009:293, paragraph 59.

2.4 Transfer of personal data to third countries

The investigation shows that the data collected through the Tool is stored by Google LLC in the United States. Thus, the personal data collected through the Tool is transferred to the United States.

The question is whether Dagens Industri's transfer of personal data to the United States complies with Article 44 of the GDPR and has legal support for it in Chapter V.

2.4.1 Applicable provisions, etc.

Article 44 of the GDPR, entitled 'General principle for the transfer of data', provides, *inter alia*, that transfers of personal data which are under processing or are intended to be processed after their transfer to a third country — i.e. a country outside the EU/EEA — may take place only if, subject to the other provisions of the GDPR, the controller and processor fulfil the conditions set out in Chapter V. All provisions of that chapter are to be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

Chapter V of the GDPR contains tools that can be used for transfers to third countries to ensure a level of protection that is essentially equivalent to that guaranteed within the EU/EEA. This could include, for example, transfers based on an adequacy decision (Article 45) and transfers subject to appropriate safeguards (Article 46). In addition, there are derogations for specific situations (Article 49).

In Schrems II, the Court of Justice of the European Union annulled the adequacy decision previously in force in respect of the United States.¹⁷ In the absence of an adequacy decision since July 2020, cannot transfers to the United States be based on Article 45.

Article 46(1) provides, *inter alia*, that in the absence of a decision in accordance with Article 45(3), a controller or processor may only transfer personal data to a third country after having taken appropriate safeguards, and subject to the availability of statutory rights of data subjects and effective remedies for data subjects. Article 46(2)(c) provides that such appropriate safeguards may take the form of standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).

In Schrems II, the Court of Justice did not reject standard contractual clauses as a transfer tool. However, the Court found that they are not binding on the authorities of the third country. In that regard, the Court held that '*Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.*'¹⁸

¹⁷ 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 Privacy Shield of the European Union and the United States and the judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

¹⁸ Points 125-126.

The reason why the Court of Justice of the European Union annulled the adequacy decision with the US was how the U.S. intelligence agencies can access personal data. According to the Court of Justice, the conclusion of standard contractual clauses cannot in itself ensure a level of protection required by Article 44 of the GDPR, as the safeguards set out therein do not apply when such authorities request access. The Court of Justice of the European Union therefore stated:

'It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection'.¹⁹

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgment²⁰ clarify that if the assessment of the law and practice of the third country means that the protection guaranteed by the transfer tool cannot be maintained in practice, the exporter must, in the context of his transfer, as a rule either suspend the transfer or take appropriate supplementary measures. In that regard, the EDPB notes that '*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it - by itself or in combination with others - addresses the specific deficiencies identified in your assessment of the situation in the third country as regards its laws and practices applicable to your transfer. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.*'²¹

The recommendations of the EDPB show that such supplementary measures can be divided into three categories: contractual, organisational and technical.²²

As regards *contractual* measures, the EDPB states that such measures "*In some situations, these measures may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country" [...] Provided the nature of contractual measures, generally not capable of binding the authorities of that third country when they are not party to the contract, these measures may often need to be combined with other technical and organisational measures to provide the level of data protection required [...]*".²³

With regard to *organisational* measures, the EDPB stresses "[a] electing and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. Depending on the specific circumstances of the transfer and the assessment performed on the legislation of the third country, organisational measures are needed to complement contractual and/or technical measures, in order to ensure a level of

¹⁹ Paragraph 133.

²⁰ 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 (hereinafter "EDPB Recommendations 01/2020").

²¹ EDPB Recommendations 01/2020, item 75.

²² EDPB Recommendations 01/2020, item 52.

²³ EDPB Recommendations 01/2020, item 99.

protection of the personal data essentially equivalent to that guaranteed within the EEA".²⁴

With regard to *technical measures*, the EDPB points out that '*measures, which may supplement safeguards found in Article 46 GDPR transfer tools to ensure compliance with the level of protection required under EU law in the context of a transfer of personal data to a third country*'.²⁵ The EDPB states in this regard that "*The measures listed below are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. These measures would be necessary to guarantee an essentially equivalent level of protection to that guaranteed in the EEA, even if the public authorities' access complies with the law of the importer's country, where, in practice, such access goes beyond what is necessary and proportionate in a democratic society.*²⁶ *These measures aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts*".²⁶

2.4.2 Assessment by the Swedish Authority for Privacy Protection (IMY)

2.4.2.1 Applicable transfer tool

The investigation shows that Dagens Industri and Google have entered into standard data protection clauses (standard contractual clauses) within the meaning of Article 46 of the GDPR for the transfer of personal data to the United States. These clauses are in line with those published by the European Commission in Decision 2010/87/EU and thus a transfer tool under Chapter V of the GDPR.

2.4.2.2 Legislation and situation in the third country

As can be seen from the judgment in Schrems II, the use of standard contractual clauses may require supplementary measures. Therefore, an analysis of the legislation of the third country in question needs to be carried out.

IMY considers that the analysis already carried out by the Court of Justice of the European Union in Schrems II, which relates to similar circumstances, is relevant and topical, and that it can therefore serve as a basis for the assessment in the case without further analysis of the legal situation in the United States.

Google LLC, as an importer of the data to the United States, shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881(b)(4). Google is therefore subject to surveillance by U.S. intelligence agencies pursuant to 50 US § 1881a ("702 FISA") and is therefore obliged to provide the U.S. government with personal data when 702 FISA is used.

In Schrems II, the Court of Justice of the European Union held that the US surveillance programmes based on 702 FISA, Executive Order 12333 (hereinafter 'E.O. 12333') and Presidential Policy Directive 28 (hereinafter 'PPD-28') do not meet the minimum requirements laid down in EU law in accordance with the principle of proportionality. This means that the monitoring programmes based on those provisions cannot be considered to be limited to what is strictly necessary. In addition, the Court found that

²⁴ EDPB Recommendations 01/2020, item 128.

²⁵ EDPB Recommendations 01/2020, item 77.

²⁶ EDPB Recommendations 01/2020, item 79.

the monitoring programmes do not confer rights on data subjects that may be invoked against US authorities in court, which means that those persons do not have the right to an effective remedy.²⁷

Against this background, IMY notes that the use of the European Commission's standard contractual clauses is not in itself sufficient to achieve an acceptable level of protection for the transferred personal data.

2.4.2.3 Supplementary measures implemented by Google and Dagens Industri

The next question is whether Dagens Industri has taken sufficient additional protective measures.

As data controller and exporter of personal data, Dagens Industri is obliged to ensure that the rules in the GDPR are complied with. This responsibility includes, *inter alia*, assessing, on a case-by-case basis, in the case of transfers of personal data to third countries, which supplementary measures are to be used and to what extent, including assessing whether the measures taken by the recipient (Google) and the exporter (Dagens Industri) taken together are sufficient to achieve an acceptable level of protection.

2.4.2.3.1 Google's supplementary measures

Google LLC, as an importer of personal data, has taken contractual, organisational and technical measures to supplement the standard contractual clauses. In its opinion on 9 April 2021, Google stated that it had taken action.

The question is whether the supplementary measures taken by Dagens Industri and Google LLC are effective, in other words, hindering U.S. intelligence services' ability to access the transferred personal data.

As regards the *legal and organisational measures*, it can be noted that neither information to users of the Tool (such as Dagens Industri), the²⁸ publication of a transparency report or a publicly available "government enquiries policy" prevents or reduces the ability of U.S. intelligence agencies to access the personal data. In addition, it is not described what it means that Google LLC's "*scrupulous review*" of any "*legality*" request from U.S. intelligence agencies. IMY notes that this does not affect the legality of such requests as, according to the CJEU, they are not compatible with the requirements of EU data protection rules.

As regards the *technical measures* taken, neither Google LLC nor Dagens Industri have clarified how the described measures — such as the protection of communications between Google services, the protection of data when transferring between data centres, the protection of communications between users and websites, or "*physical security*" — prevent or reduce the ability of U.S. intelligence services to access the data under the US regulatory framework.

With regard to the encryption technology used for example, for so-called "*data at rest*" ("*data at rest*") in data centers, which Google LLC mentions as a technical measure, Google LLC as an importer of personal data nevertheless has an obligation to grant access to or supply imported personal data held by Google LLC, including any encryption keys necessary to make the data understandable.²⁹ Thus, such a technical

²⁷ Paragraphs 184 and 192. Paragraph 259 et seq.

²⁸ Regardless of whether such a notification would even be permitted under U.S. law.

²⁹ See EDPB Recommendations 01/2020, paragraph 81.

measure cannot be considered effective as long as Google LLC is able to access the personal data in plain language.

As regards Google LLC's argument that '*to the extent that data for measurement in Google Analytics transmitted by website holders constitute personal data, they may be regarded as pseudonymised*', it can be concluded that Universal Unique Identifiers (UUIDs) are not covered by the concept of pseudonymisation in Article 4(5) of the GDPR. Pseudonymisation can be a privacy-enhancing technology, but the unique identifiers, as described above, have the specific purpose of distinguishing users and not serving as protection. In addition, individual identification is made through what has been stated above about the ability to combine unique identifiers and other data (e.g. metadata from browsers or devices and the IP address) and the ability to link such information to a Google account for logged-in users

With regard to Google's action relating to the anonymisation of IP addresses in the form of truncation³⁰, it is not apparent from Google's response whether this action takes place prior to transmission, or whether the full IP address is transmitted to the United States and shortened only after transmission to the United States. From a technical point of view, it has therefore not been shown that there is no potential access to the entire IP address before the last octet is truncated.

With regard to the fact that Google LLC has configured the solution so that the JavaScript file is cached in the application cache of the receiving terminal for two hours (which may mean a delay between the first and second call of up to two hours), this means that the calls may have different time stamps, which could in itself amount to an aggravation of the identification of which visitor has made the unique call. IMY notes, however, that Dagens Industri cannot ensure that a delay in the calls actually occurs, partly because it is technically impossible to ensure when (or if) a delay between the first and second call occurs, and when the control (activation) of the caching is beyond the company's control.

Against this background, IMY concludes that the supplementary measures put in place by Google are not effective, as they do not prevent US intelligence services from accessing the personal data or rendering such access ineffective.

2.4.2.3.2 Dagens Industri's own supplementary measures

Dagens Industri has stated that it has taken supplementary measures in addition to the measures taken by Google. These consist, according to Dagens Industri, that the company has carried out extensive mapping of the life cycle of personal data processed in the Tool and that the company on its own data servers (*transmission through the proxy server*) masks the last octet of the IP address and has the value of the cookies before the data is transferred to Google.³¹

However, IMY considers that these measures are not sufficient for the following reasons.

It is apparent from the company's own data that *two separate* transfers of the individual's IP address are made to Google LLC — *partly* through a call from *the measurement tool "analytics.js"* with the entire IP address exposed and *partly*³² by

³⁰ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

³¹ See above in the section on the company's submissions, under the heading 'Additional protective measures taken'.

³² Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this action means

truncating the last octet when the measured data is transmitted (*and hashing of the cookie value*).³³

Dagens Industri argues that what can be seen from the first transmission (where the entire IP address is exposed) is only the web page that the IP address has visited and that it is not possible to link the IP address with the page view data etc. which is later measured on the Website. However, IMY notes that the transfer itself involves the transfer of a personal data (IP address), despite the safeguards taken.

With regard to the second transmission, it also contains additional information about the visit to Dagens Industri's website (such as the visitor's device and the time of the visit) and the connection should therefore be made with the IP address as the difference after truncation is only that the last octet is masked, which for IP addresses means only 256 options (i.e. a number between 0-255). Although the masking of the last octet and the "hashing" of the cookie value constitute privacy-enhancing measures, as they limit the scope of the data that authorities can access (in third countries), IMY notes that it is nevertheless possible to link the transferred data to other data which are also transferred to Google LLC.

Against this background, IMY also finds that the supplementary measures taken by it, in addition to the supplementary measures taken by Google, are not effective enough to prevent US intelligence services from accessing the personal data or rendering such access ineffective.

2.4.2.3.3 Conclusion of the Swedish Authority for Privacy Protection (IMY)

IMY finds that Dagens Industri's and Google's actions are neither individually nor collectively effective enough to prevent U.S. intelligence services from accessing the personal data or rendering such access ineffective.

Against this background, IMY considers that neither standard contractual clauses nor the other measures invoked by Dagens Industri can provide support for the transfer as set out in Chapter V of the GDPR.

With this transfer of data, Dagens Industri therefore undermines the level of protection of personal data for data subjects guaranteed by Article 44 of the GDPR.

IMY therefore concludes that Dagens Industri Aktiebolag violates Article 44 of the GDPR.

3 Choice of intervention

3.1 Applicable provisions

In case of breaches of the GDPR, IMY has a number of corrective powers available under Article 58(2)(a) to (j) of the GDPR, including reprimand, orders and administrative fines.

that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.

³³ See above in section 1.3.17.1, illustration of data flows (p. 8 of the company's opinion).

IMY shall impose fines in addition to or in place of other corrective measures referred to in Article 58(2), depending on the circumstances of each case.

Each supervisory authority shall ensure that the imposition of administrative fines on a case-by-case basis is effective, proportionate and dissuasive. This is set out in Article 83(1) of the GDPR.

Article 83(2) of the GDPR sets out the factors to be considered in determining whether an administrative fine is to be imposed, but also in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing an administrative fine, issue a reprimand under Article 58(2)(b) of the Regulation. Account must be taken of aggravating and mitigating factors in the case, such as the nature, gravity and duration of the infringement and the relevant past infringements.

Pursuant to Article 83(5)(c) GDPR, in the event of a breach of Article 44 pursuant to Article 83(2), administrative fines of up to EUR 20 million or, in the case of an undertaking, up to 4 % of the total global annual turnover in the previous financial year, whichever is higher, are to be imposed.

3.2 Should an administrative fine be imposed?

IMY has found above that the transfers of personal data to the United States that take place through the Google Analytics tool and for which Dagens Industri is responsible are in breach of Article 44 of the GDPR. Infringements of that provision may, as stated above, give rise to administrative fines. In the present case, it is a serious infringement which should normally be subject to an administrative fine.

When assessing whether a fine should be imposed in this case, account must be taken, in *aggravatingly factor*, of the fact that Dagens Industri has transferred a large amount of personal data to a third country where the data cannot be guaranteed the level of protection afforded in the EU/EEA. The treatment has been carried out systematically and for a long time. Following the Court of Justice of the European Union's judgment of 16 July 2020, the Commission's adequacy decision in the United States³⁴ changed the conditions for transfers of personal data to the United States. It has now elapsed around 3 years since the judgment was delivered and the EDPB has, during that time, made recommendations on the impact of the public consultation ruling on 10 November 2020 and in final form on 18 June 2021.

In *mitigating factor*, account must be taken of the specific situation arising after the judgment and the interpretation of the EDPB's recommendations, where there has been a gap after the transfer tool to the United States has been rejected by the Court of Justice of the European Union, according to the Commission's previous decision. It should also be taken into account in particular that the investigation shows that Dagens Industri has made a serious analysis and mapping of the life cycle of personal-data in the Tool. Dagens Industri has also taken steps such as that the company on its own data servers (transmission through the proxy server) masks the last octet of the IP address (trunking) and has the value of the cookies before the data is transferred to Google. The company has also activated Google's "anonymisation of IP addresses" action by truncation. Dagens Industri has thus taken relatively extensive measures to try to limit the risks to the data subjects and to heal the shortcomings. Dagens Industri

³⁴ 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-US Privacy Shield.

has thus also believed that they have succeeded even if the measures in practice have now proved to be not effective.

On a weight of evidence assessment, IMY finds that there is reason to refrain in this case from imposing administrative fine on Dagens Industri for the infringement found and to stay at an order to rectify the deficiency.

3.3 Other interventions

The investigation shows that the transfer measures relied on by Dagens Industri cannot support the transfer under Chapter V of the GDPR. The transfer therefore infringes the Regulation. In order to ensure that the infringement is brought to an end, Dagens Industri shall be ordered pursuant to Article 58(2)(d) of the GDPR to ensure that the Company's processing of personal data in the context of the use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, Dagens Industri ceases to use the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards have been taken. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

4 How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

This decision was taken by Director-General [REDACTED] following a presentation by the legal advisors [REDACTED]. [REDACTED], Head of Legal Affairs, [REDACTED], Head of Unit, and information security specialist [REDACTED]. [REDACTED] have also participated in the final proceedings.

Summary Final Decision Art 60

Complaint

EDPBI:SE:OSS:D:2023:790

Violation identified, Administrative fine

Background information

Date of complaint:	27 May 2018
Draft decision:	N/A
Revised draft decision:	N/A
Date of final decision:	12 June 2023
Date of broadcast:	12 June 2023
Controller:	Spotify AB
Processor:	N/A
LSA:	SE
CSAs:	All SAs
Legal Reference(s):	Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 15 (Right to access by the data subject).
Decision:	Violation identified, Administrative fine.
Key words:	Data subject rights, Data retention, Right of access, Retention time, Administrative fine.

Summary of the Decision

Origin of the case

Due to complaints that the LSA received against the controller regarding the right of access pursuant to Article 15 of the GDPR, the LSA initiated supervision against the controller.

The first complainant submitted that, with regards to his request of access made on 27 May 2018, the controller had not granted access to all his personal data within the period laid down in Article 12(3) of the GDPR and that, once he had obtained access to all personal data, it had not been provided in an intelligible form as provided for in Article 12(1) of the GDPR.

The second complainant submitted that, with regard to his request for access made on 10 October 2018, the controller had not provided all the personal data it processed about the complainant, that the controller had not provided any of the information concerning the processing of the complainant's personal data required by Article 15(1)(a) to (h) and (2) of the GDPR, and that the controller had not

provided the personal data in an intelligible form as provided for in Article 12(1) of the GDPR. In that regard, the complainant stated, inter alia, that the data were provided in a format which was only machine-readable and not comprehensible to natural persons.

The third complainant claimed that the controller had not responded to the complainant's request of access under Article 15 of the GDPR made on 12 November 2018.

Findings

The LSA considered that the controller had not provided sufficiently clear information about the purposes of the processing (**Article 15(1)(a)** GDPR), the categories of personal data concerned (**Article 15(1)(b)** GDPR), recipients or categories of recipients (**Article 15(1)(c)** GDPR) or the source from which the data were collected (**Article 15(1)(g)** GDPR). The information was not concise, and transparent, nor easily accessible and did not meet the requirements of **Article 12(1)** of the GDPR.

Moreover, the LSA considered that the information provided concerning retention periods did not meet the requirements of **Article 15(1)(d)** of the GDPR. Also in this case, the information was not concise and transparent, nor easily accessible and it did not meet the requirements of **Article 12(1)** of the GDPR. The LSA therefore considered that the information provided regarding third country transfers did not meet the requirements of **Article 15(2)** GDPR. The information was not concise and transparent, nor easily accessible and it did not meet the requirements of **Article 12(1)** of the GDPR.

The LSA found that the description of the data contained in the technical log files provided by the controller during the period from 11 June 2019 to 16 May 2022 had not complied with the requirements of Article 12(1) of the GDPR as this information had been provided by default only in English. The controller had therefore processed personal data in breach of **Article 12(1)** of the GDPR during the period in question.

For the first complaint, the LSA considered that the controller had processed personal data in breach of **Article 12(3)** of the GDPR, by not having provided the copy of personal data in due time, and in breach of Articles **12(1), 15(1)** and **15(3)** of the GDPR, by not having provided all of the complainant's personal data in an intelligible form. For the second complaint, the LSA considered that the controller had processed personal data in breach of **Article 15(1)** and **(3)** of the GDPR, by not having given access to all the personal data that the controller processed about the complainant and in breach of **Article 15(1)(a) to (h)** and **(2)** of the GDPR, by not providing any of the information specified in these provisions. For the third complaint, the investigation had not shown that the controller had failed in its handling of the complainant's request for access, with the result that the complaint in question should have been rejected. The receiving supervisory authority, the DK SA, was responsible for adopting the decision with regard to this complaint under Article 60(8) GDPR.

Decision

The controller had processed personal data in breach of Articles 12(1), 15(1)(a) to (d), 15(1)(g) and 15(2) of the GDPR. The LSA decided that the controller shall pay an administrative fine of 58,000,000 (fifty-eight million) SEK for these infringements.

The LSA found, with regard to the first complaint, that the controller had processed personal data in violation of Articles 12(1), 12(3), 15(1) and 15(3) of the GDPR. The LSA found, with regard to the second complaint, that the controller had processed personal data in violation of articles 15(1) and 15(3) of the GDPR and of articles 15(1)(a) to (h) and 15(2) GDPR. The LSA issued a reprimand to the controller pursuant to Article 58(2)(b) of the GDPR for the infringements relating to the first two complaints. Pursuant to Article 58(2)(c) of the GDPR, the LSA ordered the controller to comply with the complainant's request for access in respect of the second complaint. This measure shall have been implemented no later than one month after this decision had become final.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision in case with national reference number, DI-2020-11397. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2020-11397

Date of decision:
2023-06-30

Final decision under the General Data Protection Regulation– CDON AB transfers of personal data to third countries

Table of contents

Decision of the Swedish Authority for Privacy Protection (IMY)	3
1. Report on the supervisory case	3
1.1 Processing	3
1.2 What is stated in the complaint	4
1.3 What CDON has stated.....	4
1.3.1 Who has implemented the Tool and for what purpose etc.	4
1.3.2 Recipients of the data.....	5
1.3.3 The data processed in the Tool and what constitutes personal data	5
1.3.4 Categories of persons concerned by the treatment	5
1.3.5 When the code for the Tool is executed and recipients are accessed	5
1.3.6 How long the personal data are stored	5
1.3.7 The countries in which personal data are processed	6
1.3.8 CDON's relationship with Google LLC	6
1.3.9 Ensure that processing is not carried out for the purposes of the recipients	6
1.3.10 Description of CDON's use of the Tool	6
1.3.11 Own checks on transfers affected by the judgment in Schrems II	6
1.3.12 Transfer tools under Chapter V of the GDPR.....	7
1.3.13 Verification of obstacles to compliance in third country legislation	7
1.3.14 What information is covered by the definition of personal data....	7
1.3.15 Effectiveness of measure taken by Google and CDON	8

Mailing address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

1.4 What Google LLC has stated	8
1.5 CDON's comment on Google's opinion	10
2 Statement of reasons for the decision	10
2.1 The framework for the audit	10
2.2 This is the processing of personal data.....	11
2.2.1 Applicable provisions, etc.....	11
2.2.2 Assessment of the Swedish Authority for Privacy Protection (IMY)	12
2.3 CDON is the data controller for the processing.....	15
2.4 Transfer of personal data to third countries	15
2.4.1 Applicable provisions, etc.....	15
2.4.2 Assessment of the Swedish Authority for Privacy Protection (IMY)	17
3 Choice of intervention	21
3.1 Legal regulation.....	21
3.2 Should an administrative fine be imposed?	21
3.3 Other interventions.....	24
4 How to appeal	25

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection finds that the investigation has shown that CDON AB processed personal data in breach of Article 44 of the GDPR¹ by using the Google Analytics tool provided by Google LLC on its website www.cdon.fi, and thus transferring personal data to third countries without fulfilling the conditions laid down in Chapter V of the Regulation, since 14 August 2020 and until the date of this Decision.

Pursuant to Article 58(2)(d) of the GDPR, CDON AB is required to ensure that the company's processing of personal data in the context of the company's use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V of the GDPR. In particular, CDON AB shall cease to use the version of the Google Analytics tool used on 14 August 2020, unless sufficient safeguards have been taken. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

On the basis of Articles 58(2) and 83 of the GDPR, IMY decides that CDON AB shall pay an administrative fine of SEK 300 000 (three hundred thousand) for infringement of Article 44 of the GDPR.

1. Report on the supervisory case

1.1 Processing

The Swedish Integrity Authority for Protection Authority (IMY) has initiated supervision regarding CDON AB (hereinafter CDON or the company) due to a complaint. The complaint has claimed a breach of the provisions of Chapter V of the GDPR related to the transfer of the complainant's personal data to third countries. The transfer is alleged to have taken place when the complainant visited the company's website, www.cdon.fi (hereinafter "the company's website" or the "Website") through the Google Analytics tool (hereinafter the Tool) provided by Google LLC.

The complaint has been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainant has lodged their complaint (Austria) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned are the data protection authorities in Germany, Norway, Estonia, Denmark, Portugal, Spain, Finland and Austria.

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).

1.2 What is stated in the complaint

The complaint has essentially stated the following.

On 14 August 2020 the complainant visited the CDON website. The complainant visited the controller's website, while being logged in to the Google/ Facebook account associated with the complainant's email address. On the website, the controller has embedded a JavaScript code for Google/ Facebook services including "Google Analytics" or "Facebook Connect". In accordance with paragraph 5.1.1(b) of the terms and conditions of Google's processing of personal data for Google's advertising products and also Google's terms and conditions for processing the New Google Ads Processing Terms, for Google Advertising Products, Google processes personal data on behalf of the controller (i.e. CDON) and is therefore to be classified as the company's data processor.

During the visit of the company's website, CDON processed the complainant's personal data, at least the complainant's IP address and the data collected through cookies. Some of the data has been transferred to Google. In accordance with Section 10 of the Terms and Conditions on the Processing of Personal Data for Google's Advertising Products, CDON has authorised Google to process personal data of the Applicant in the United States. Such transfer of data requires legal support in accordance with Chapter V of the GDPR.

According to the judgment of the Court of Justice of the European Union (CJEU), in Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)², the company could no longer rely on an adequacy decision under Article 45 of the GDPR for the transfer of data to the United States. CDON should not base the transfer of data on standard data protection clauses under Article 46(2)(c) GDPR if the recipient of the personal data in the third country does not ensure appropriate protection with regard to Union law for the personal data transferred.

Google shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881 (4)(b) and is thus subject to surveillance by U.S. intelligence services in accordance with 50 US § 1881a (Section 702 of the Foreign Intelligence Surveillance Act, below "702 FISA").³ Google provides the U.S. government with personal data in accordance with these provisions. CDON cannot therefore ensure adequate protection of the complainant's personal data when it is transmitted to Google.

1.3 What CDON has stated

CDON AB have in opinions on the 15 January 2021, 15 February 2022 and 31 August 2022, essentially stated the following.

1.3.1 Who has implemented the Tool and for what purpose etc.

The code for the Tool was embedded on the Website at the time of the complaint and is still embedded on the Website. The decision to embed the Tool on the Website was made by CDON, a company registered in Sweden. Data is collected from all persons

² Judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

³ See <https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881.htm> and <https://www.govinfo.gov/content/pkg/USCODE-2011-title50/html/USCODE-2011-title50-chap36-subchapVI-sec1881a.htm>.

visiting the Website, which is likely to include data subjects from more than one EU/EEA Member State.

CDON uses the Tool to get to know the traffic and uses the Website to make various business-critical decisions. It is possible to find out which product categories are most popular and how customers navigate, partly to find CDON and to end a purchase.

1.3.2 Recipients of the data

In the context of CDON's use of the Tool on the Website, personal data is only disclosed to Google.

1.3.3 The data processed in the Tool and what constitutes personal data

The data processed in the context of CDON's use of the Tool are different characteristics or actions taken by the visitor on the Website, such as:

1. What elements the user has seen while navigating and looking around the Site,
2. Clicked on an Image/Banner on the Website,
3. Added or removed something to the cart,
4. Came to checkout or completed a purchase,
5. Clicked on suggestions for accessories on product pages or added something to the wishlist,
6. If the user is a member of the CDON customer club; and
7. The search string used by the user to search internally on the Website.

In addition to this data, Google also has access to the IP address of the respective user.

1.3.4 Categories of persons concerned by the treatment

The categories of persons concerned by the processing are all categories of persons who visit the Website. CDON has no means of distinguishing if data on particularly vulnerable persons are processed. This is because CDON only processes anonymous "behavioural data" regarding how a user navigates the Website. The information processed by CDON is no more than the transfer of the information to Google. CDON cannot identify individual users before or after disclosure to Google. The category of persons a unique user belongs to is therefore unknown to CDON.

1.3.5 When the code for the Tool is executed and recipients are accessed

Immediately after the Website has finished loading into the user's browser, information about the location of the user on the Website has been transmitted to Google. Since 12 January 2021, CDON has activated a tool that requires the respective user's consent to integrate and run the content of the Tool into the user's browser.

1.3.6 How long the personal data are stored

Data and other information are not stored by CDON, but are transmitted by CDON to Google in real time. CDON's assessment is that the anonymisation of IP addresses described below means the data transferred to Google can no longer be linked to a specific individual and are therefore not personal data. Google will only store personal

data until the IP addresses are truncated⁴. According to Google, truncation is executed as soon as technically possible.

1.3.7 The countries in which personal data are processed

The data transmitted to the Tool is stored, for example in the United States.

1.3.8 CDON's relationship with Google LLC

CDON share the assessment made by Google regarding the allocation of personal data, whereby Google is deemed to process data in the context of CDON's use of the Tool as a data processor for CDON. CDON acts as data controller.

The terms that apply to the tool are both Google's Terms of Service and Google's data processing terms.

The sharing of personal data by Google and CDON is set out in the Google Ads Data Processing Terms.

1.3.9 Ensure that processing is not carried out for the purposes of the recipients

CDON has not had any reason to assume that Google does not meet the requirements of the Google Ads Data Processing Terms, so that its compliance with those terms has not yet been further verified by CDON.

1.3.10 Description of CDON's use of the Tool

CDON uses the Tool in order to get to know the traffic on the Website and to be able to make various business-critical decisions based on that information. For example, it is possible to find out which product categories are most popular and how customers navigate the Website to find CDON and to end a purchase.

1.3.11 Own checks on transfers affected by the judgment in Schrems II

Following the Schrems II judgment, CDON has taken measures in the form of identifying which of CDON's partners are located in countries outside the EU/EEA and, in relation to the respective partners, requested information on the additional security measures they have taken as a result of the ruling.

On October 26, 2020, CDON requested information from Google regarding the effect of CDON's embedding of the Code for the Tool on the Website. Google has not returned in response to CDON's request for information and, for this reason, in addition to repeating the request to Google and reminding of replies, CDON has sought publicly available information on the actions taken by Google as a result of the ruling.

According to publicly available information from Google, in addition to the Standard Contractual Clauses, Google has taken the following additional safeguards in relation to the Tool:

- Google ensures the secure transfer of JavaScript libraries and measurement data using the HTTP HSTS (Strict Transport Security) encryption protocol.
- The Tool has been certified according to the internationally accepted independent safety standards ISO 27001.

⁴ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

In addition to these actions, CDON has also chosen to activate IP anonymisation in the code of the tool, which means that IP addresses are truncated. IP anonymisation means that the last octet of IPv4 addresses and the last 80 bits of IPv6 addresses are deleted immediately after the addresses have been sent to the Tool Collection Network. Since CDON's view is that it is the IP addresses that cause the other data collected and transmitted using the Tool to be considered personal data, CDON's assessment is that the truncation of the IP addresses means that no information transmitted to Google is considered personal data after the IP anonymisation/trunking has been carried out.

1.3.12 Transfer tools under Chapter V of the GDPR

Transfers of personal data to recipients in third countries under CDON's use of the Tool are carried out on the basis of the European Commission's Standard Contractual Clauses (2010/87/EU).

In accordance with the versions of Google's data processing terms in force since 12 August 2020, Google and CDON have entered into EU Standard Contractual Clauses for the transfer of data from an EU controller to a data processor outside the EU, based on template 2010/87/EU of the European Commission.

1.3.13 Verification of obstacles to compliance in third country legislation

In order to ensure compliance with the contractual obligations set out in the standard contractual clauses, CDON has sent the request for information to Google regarding third country transfer described above and CDON has received no reply.

1.3.14 What information is covered by the definition of personal data

It is important to distinguish between the concepts of being able to distinguish users and not being able to identify a specific individual. The latter, identification of a specific individual is not the purpose of the use of the Tool, nor is it possible with the information collected by unique identifiers (which may be derived from the browser or device (i.e. CDON's Google Analytics account ID)) neither alone nor in combination with, *inter alia*, the information generated during visits to the Website (i.e. Web address (URL) and HTML title on that Website or browser information). CDON is of the firm opinion that IP addresses are necessary to process, among other things, the information generated when visiting the Website (i.e. URL (URL) and HTML title on that Website or information about browsers) may be considered personal data. CDON acknowledges that in certain circumstances dynamic IP addresses may be considered personal data. However, the differentiation of users made possible by the information collected by unique identifiers is not sufficient for a specific individual to be identified, with or without means such as, for example, disclosure, but only in combination with a full IP address that the information collected by unique identifiers and information generated by visits to the Website may constitute personal data.

The judgments Breyer⁵ and M.I.C.M.⁶ support the assessment that dynamic IP addresses are, in all cases, personal data. According to the Court of Justice, dynamic IP addresses may be regarded as personal data in relation to the provider of information or communication services concerned, not in relation to any operator accessing an IP address. In the judgement Breyer, concerning the assessment of the means which could reasonably be used to identify the person concerned, the Court held that, under German law, there were legal means enabling the provider of

⁵ Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:C:2016:779.

⁶ Judgment of the Court of Justice of the European Union M.I.C.M., C-597/19, EU:C:2021:492.

electronic information or communications services, in particular in the event of cyber attacks, to apply to the competent authority in order to take the necessary steps to obtain such information from the internet service provider and to initiate criminal proceedings. It may be questioned whether a U.S. authority with a truncated IP address, which may constitute one of 256 alternative IP addresses, has such lawful means as may reasonably be used to enable the identification of an individual, when, in the case of Breyer, a full IP address was even considered problematic in relation to the actual provider of that natural person's IT services.

1.3.15 Effectiveness of measure taken by Google and CDON

With reference to the answers above, in addition to the activation of IP anonymisation, CDON has not considered the implementation of accompanying measures as Google has informed that additional measures have been taken.

The truncation of IP addresses is an effective protection measure. Regardless of whether the IP addresses are truncated in connection with, or in connection with, the transmission of the information from CDON to Google. The truncation of the IP addresses means that the information stored on Google's servers in the United States does not constitute personal data. In a situation where the truncation takes place only after the data has been received by Google LCC, but at the latest immediately after receipt, the truncation means that all the data transmitted by CDON to Google and stored on Google's servers will not constitute personal data because the IP address, which is the unique identifier that causes the other information transmitted to constitute personal data, has been anonymised. The IP address without the last octet may be any of 256 alternative IP addresses and therefore a truncated IP address by thinning together with other information cannot be considered personal data.

1.3.16 Supplementary measures taken in addition to those taken by Google

During the handling of the case, CDON has thoroughly analysed and investigated the possibilities of switching to another solution that does not involve the use of the Tool. CDON have done preparations for such a change, which it will hopefully be able to implement promptly if IMY's final decision indicates that the Tool is not compliant with the GDPR and when that kind of decision becomes final. CDON's analysis shows that such a change (i.e. switch to a different solution) will be very burdensome for the company (in particular in comparison with other market players), so that it cannot be implemented before there is clarity in relation to what applies to the Tool as to what is a supplementary measure.

1.4 What Google LLC has stated

IMY has added to the case an opinion of Google LLC (Google) on 9 April 2021 submitted by Google to the data protection authority in Austria. The opinion answers questions asked by IMY and a number of regulators to Google in response to partial joint handling of similar complaints received by these authorities. CDON has been given the opportunity to comment on Google's opinion. Google's opinion shows the following about the Tool.

A JavaScript code is included on a web page. When a user visits (calls) a web page, the code triggers a download of a JavaScript file. After that, the Tool tracking operation, which consists of collecting information related to the call in different ways and sending the information to the server of the Tool, is performed.

A website manager who integrated the Tool on his website may send instructions to Google for the processing of the data collected. These instructions are transmitted via the so-called tag manager who manages the tracking code that the webmaster has integrated into his website and through the tag manager's settings. The person who integrated the tool can make different settings, for example regarding storage time. The Tool also enables those who integrated it to monitor and maintain the stability of their website, for example by keeping themselves informed of events such as peaks in visitor traffic or lack of traffic. The Tool also enables a website manager to measure and optimise the effectiveness of advertising campaigns carried out using other Google tools.

In this context, the Tool collects visitor's http calls and information about, among other things, the visitor's browser and operating system. According to Google, a http call for any page contains information about the browser and device making the call, such as domain names, and information about the browser, such as type, reference and language. The Tool stores and reads cookies in the visitor's browser to evaluate the visitor's session and other information about the call. Through these cookies, the Tool enables unique users identification (UUID) over browsing sessions, but the Tool cannot identify unique users in different browsers or devices. If a site owner's website has its own authentication system, the site owner can use the ID feature to identify a user more accurately on all the devices and browsers they use to access the site. When the information is collected, it is transferred to the servers of the Tool. All data collected through the Tool is stored in the United States.

Google has put in place, among other things, the following legal, organisational and technical measures to regulate transfers of data within the framework of the Tool.

Google has put in place legal and organisational measures, such as that it always conducts a thorough review of a request for access from government authorities if user data can be implemented. It is lawyers/specially trained staff who conduct these trials and investigate whether such a request is compatible with applicable laws and Google's guidelines. Data subjects are informed of the disclosure, unless prohibited by law or would adversely affect an emergency. Google has also published a policy on its website on how to implement such a request for access by government authorities of user data.

Google has put in place technical measures such as protecting personal data from interception when transmitting data in the Tool. By default using HTTP Strict Transport Security (HSTS), which instructs browsers such as http to SSL (HTTPS) to use an encryption protocol for all communication between end-users, websites, and tool servers. Such encryption prevents intruders from passively listening by communications between websites and users.

Google also uses encryption technology to protect personal data known as "data at rest" in data centers, where user data is stored on a disk or backup media to prevent unauthorised access to the data.

In addition to the above actions, website owners may use IP anonymisation by using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated and contribute to data minimisation. If the IP anonymisation service is fully used, the anonymisation of the IP address takes place almost immediately after the request has been received.

Google also restricts access to the data from the Tool through permission control and by all personnel having completed information security training.

1.5 CDON's comment on Google's opinion

CDON maintains what was stated in the opinion of 15 January 2021. In addition, CDON presents the following in response to Google's opinion of 9 April 2021.

In its use of the Tool, CDON has taken the security measures provided by the Tool.

Google's observations state, *inter alia*, as follows:

"As a general matter, unless instructed to do so, Google does not attempt to link data it collects as a processor on behalf of website owners using Google Analytics with data it collects as a controller in relation to its users and the relevant policies and systems are designed to avoid such linking."

Google thus states that the owner of the website has full control over the personal data processed by Google by allowing users of the tool to provide Google with specific instructions to link the personal data with users. CDON has not given Google any such instructions.

CDON has instead focused on using the settings provided by the Tool to restrict Google's use of personal data. Such settings include, in particular, enabling IP anonymisation in the code of the Tool, which means that IP addresses are truncated. CDON had also limited the storage time of the personal data and has not enabled the User ID function. CDON has thus not been able to link a fixed ID of a single user to the user's engagement data from one or more sessions initiated from one or more devices.

In conclusion, CDON maintains that the use of the Tool has been carried out in accordance with the security measures offered by the Tool. It should also be noted that obligations under Chapter V of the GDPR are primarily obligations imposed on the exporter, which in this case are CDON resellers (see EDPB Guidelines 05/2021 and decisions of the data protection authority in Austria regarding Google Analytics in case 2021-0.586.257 (D155.027)).

2 Statement of reasons for the decision

2.1 The framework for the audit

Based on the complaint in the case, IMY has only examined whether CDON transfers personal data to the third country USA within the framework of the Tool and whether CDON has legal support for it in Chapter V of the GDPR. The supervision does not cover whether CDON's personal data processing otherwise complies with the General Data Protection Regulation.

2.2 This is the processing of personal data

2.2.1 Applicable provisions, etc.

In order for the GDPR to apply, personal data must be processed.

According to Article 1(2), the GDPR aims to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data. According to Article 4(1) of the GDPR personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In order to determine whether a natural person is identifiable, account should be taken of all means which, either by the controller or by another person, may reasonably be used to directly or indirectly identify the natural person (recital 26 of the GDPR).

That concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject. As regards the latter condition, it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person.⁷

The word "indirectly" in Article 4(1) of the GDPR suggests that, in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified.⁸ In addition, recital 26 of the GDPR states that in order to determine whether a natural person is identifiable, any means, such as 'singling out', which, either by the controller or by another person, may reasonably be used to directly or indirectly identify the natural person, should be taken into account. In order to determine whether devices *may reasonably be used to* identify the natural person, all objective factors, such as the cost and duration of identification, taking into account both the available technology at the time of processing, should be taken into account. According to Article 4 (5) of the GDPR, 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

So-called "net identifiers" (sometimes referred to as "online identifiers") — e.g. IP addresses or information stored in cookies — can be used to identify a user, especially when combined with other similar types of information. According to recital 30 of the GDPR, natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses, cookies or other identifiers. This may leave traces that, in particular in combination with unique identifiers and other data collected, can be used to create profiles of natural persons and identify them.

In its Breyer judgment, the Court of Justice of the European Union held that a person is not regarded as identifiable by a particular indication of whether the risk of

⁷ Judgment of the Court of Justice of the European Union Nowak, C-434/16, EU:2017:994, paragraphs 34-35.

⁸ Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:2016:779, para. 41.

identification is in practice negligible, which is whether the identification of the person concerned is prohibited by law or impossible to implement in practice.⁹ However, in the judgment in M.I.C.M. of 2021 and in the Breyer judgment, the Court of Justice of the European Union held that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of that provision, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person.¹⁰

2.2.2 Assessment of the Swedish Authority for Privacy Protection (IMY)

In order to determine whether the data processed through the Tool constitute personal data, IMY shall decide whether Google or CDON, through the implementation of the Tool, can identify individuals, e.g. the complainant, when visiting the Website or whether the risk is negligible.¹¹

IMY considers that the data processed constitute personal data for the following reasons.

The investigation shows that CDON implemented the Tool by inserting a JavaScript code (a tag), as specified by Google, into the source code of the Website. While the page loads in the visitor's browser, the JavaScript code is loaded from Google LLC's servers and runs locally in the visitor's browser. A cookie is set simultaneously in the visitor's browser and stored on the computer. The cookie contains a text file that collects information about the visitor's operation on the Website. Among other things, a unique identifier is set in the value of the cookie and this unique identifier is generated and managed by Google.

When the complainant visited the Website, or a subpage of the Website, the following information was transmitted via the JavaScript code from the complainant's browser to Google LLC's servers:

1. Unique identifier(s) that identified the browser or device used to visit the Website and a unique identifier that identified CDON (i.e. the CDON account ID for Google Analytics).
2. URL and HTML title of the website and web page visited by the complainant;
3. Information about browser, operating system, screen resolution, language setting, and date and time of access to the Website.
4. The complainant's IP address.

At the time of the complainant's visit, the identifiers referred to in paragraph 1 above were set in cookies with the names '_gads', '_ga' and '_gid' and subsequently transferred to Google LLC. Those identifiers were created with the aim of distinguishing individual visitors, such as the complainant. The unique identifiers thus make visitors to the Website identifiable. However, even if such unique identifiers (according to 1 above) were not in themselves to make individual identifiable, it must be borne in mind that, in the present case, those unique identifiers may be combined with additional elements (according to paragraphs 2 to 4 above) and that it is possible

⁹ Judgment of the Court of Justice of the European Union Breyer, C-582/14, EU:2016:779, paragraphs 45-46.

¹⁰ Judgment of the Court of Justice of the European Union M.I.C.M. C-597/19, EU:2021:492, para. 102-104, and Breyer, C-582/14; EU:C:2016:779, paragraph 49.

¹¹ See the Administrative Court of Appeal in Gothenburg's judgment of 11 November 2021 in case No 2232-21, with the agreement of the lower court.

to draw conclusions in relation to information (as set out in paragraphs 2 to 4 above) from which data constitute personal data, irrespective of whether the IP address was not transmitted in its entirety.

Combined data (according to points 1-4 above) means that individual visitors to the Website become even more separable. It is therefore possible to identify individual visitors to the Website. This in itself is sufficient for it to be considered personal data. Knowledge of the actual visitor's name or physical address is not required, as the distinction (by the word 'release' in recital 26 of the GDPR, 'singling out' in the English version) is sufficient in itself to make the visitor indirectly identifiable. Nor is it necessary for Google or CDON to identify the complainant, but the possibility of doing so is in itself sufficient to determine whether it is possible to identify a visitor. *Objective means that can reasonably be used* either by the controller or by another, are *all means that can reasonably be used* for the purpose of identifying the complainant. Examples of *objective means that can reasonably be used* are access to additional information from a third party that would allow the complainant to be identified taking into account both the available technology at the time of identification and the cost (time required) of the identification.

IMY notes that, in its judgments in M.I.C.M. and Breyer, the Court of Justice of the European Union held that dynamic IP addresses constitute personal data in relation to the person processing them, where it also has a legal means to identify the holders of internet connections using the additional information available to third parties.¹² IP addresses do not lose their character of being personal data simply because the means of identification lie with third parties. The Breyer judgment and the M.I.C.M. judgment should be interpreted on the basis of what is actually stated in the judgments, i.e. if there is a lawful possibility of access to additional information for the purpose of identifying the complainant, it is objectively clear that there is a '*legal means which enable it*' to identify the complainant. According to IMY, the judges should not be read in contrast, in such a way as to demonstrate a legally regulated possibility of access to data that could link IP addresses to natural persons in order for the IP addresses to be considered personal data. In IMY's view, an interpretation of the concept of personal data which implies that there must always be a *legal possibility* of linking such data to a natural person would constitute a significant restriction on the area of protection of the Regulation and would open up the possibility of circumventing the protection provided for in the Regulation. That interpretation would, *inter alia*, run counter to the objective of the Regulation as set out in Article 1(2) of the GDPR. The Breyer judgment is decided under Directive 95/46 previously in force and the notion of 'singling out' as set out in recital 26 of the current regulation (not requiring knowledge of the actual visitor's name or physical address, since the distinction itself is sufficient to make the visitor identifiable), was not mentioned in the previous directives as a means of identifying personal data.

In this context, there are also other data (according to paragraphs 1 to 3 above) with which the IP address can be combined to enable identification. Google's action regarding¹³ the truncation of an IP address means that the IP address can still be

¹² Judgment of the Court of Justice of the European Union M.I.C.M, C-597/19, EU:2021:492, para. 102-104 and Breyer, C-582/14

EU:C:2016:779, paragraph 49.

¹³ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this action means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information on the entity and time of visit) to third countries.

distinguished as it can be linked to other data transmitted to third countries (to the United States). This enables identification, which in itself is sufficient for the data to constitute personal data together.

In addition, several other supervisory authorities in the EU/EEA have decided that the transfer of personal data to third countries has taken place in the use of the Tool because it has been possible to combine IP addresses with other data (according to paragraphs 1 to 3 above), thus enabling the separation of data and the identification of the IP address, which in itself is sufficient to determine the processing of personal data.¹⁴

IMY notes that there may also be reasons to compare IP addresses with pseudonymised personal data. In accordance with Article 4(5) of the GDPR, pseudonymisation of personal data means that the data — like dynamic IP addresses — can no longer be attributed to a specific data subject without the use of additional information. According to recital 26 of the GDPR, such data should be considered to be data relating to an identifiable natural person.

According to IMY, a narrower interpretation of the concept of personal data would undermine the scope of the right to the protection of personal data, as guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, as it would allow controllers to specifically designate individuals together with personal data (e.g. when they visit a particular website) while denying individuals the right to protection against the dissemination of such data. Such an interpretation would undermine the level of protection of individuals and would not be compatible with the broad scope of the data protection rules laid down in the case-law of the Court of Justice of the European Union.¹⁵

Furthermore, CDON, by being logged in to its Google account when visiting the Website, processed data from which it was able to draw conclusions about the individual on the basis of his registration with Google. Google's opinion shows that the implementation of the Tool on a website makes it possible to obtain information that a user of a Google account (i.e. a data subject) has visited the website in question. It is true that Google states that certain conditions must be met in order for Google to receive such information, such as that the user (applicant) has not disabled the processing and display of personal ads. Since the applicant was logged in to its Google account when visiting the Website, Google may still have been able to obtain information about the logged-in user's visit to the Website. The fact that it is not apparent from the complaint that no personalised ads have been displayed does not mean that Google cannot obtain information about the logged-in user's visit to the Website.

In the light of the unique identifiers CAPABILITY of identifying the browser or device, the ability to derive the individual through its Google account, the dynamic IP addresses and the possibility of combining these with additional data, CDON's use of the Tool on a website, means the processing of personal data.

¹⁴ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

¹⁵ See, for example, Latvijas Republikas Saeima (Points de pénalité), C-439/19, EU:2021:504, paragraph 61; Nowak, C-434/16, EU:2017:994, paragraph 33; and Rijkeboer, C-553/07, EU:2009:293, paragraph 59.

2.3 CDON is the data controller for the processing

The controller is, among other things, the legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data (Article 4(7) GDPR). The processor is, among other things, a legal person who processes personal data on behalf of the controller (Article 4(8) GDPR).

The responses provided by CDON indicate that CDON has made the decision to implement the Tool on the Website. It also appears that CDON's purpose was to enable the company to analyse how the Website is used, in particular to be able to monitor the use of the website over time.

IMY finds that CDON, by deciding to implement the Tool on the Website for that purpose, has determined the purposes and means of the collection and subsequent transfer of this personal data. CDON is therefore the data controller for this processing.

2.4 Transfer of personal data to third countries

The investigation shows that the data collected through the Tool is stored by Google LLC in the United States. Thus, the personal data collected through the Tool is transferred to the United States.

The question is therefore whether CDON's transfer of personal data to the United States is compatible with Article 44 of the GDPR and has legal support for it in Chapter V.

2.4.1 Applicable provisions, etc.

Article 44 of the GDPR, entitled 'General principle for the transfer of data', provides, *inter alia*, that transfers of personal data which are under processing or are intended to be processed after their transfer to a third country — i.e. a country outside the EU/EEA — may take place only if, subject to the other provisions of the GDPR, the controller and processor fulfil the conditions set out in Chapter V. All provisions of that chapter are to be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.

Chapter V of the GDPR contains tools that can be used for transfers to third countries to ensure a level of protection that is essentially equivalent to that guaranteed within the EU/EEA. This could include, for example, transfers based on an adequacy decision (Article 45) and transfers subject to appropriate safeguards (Article 46). In addition, there are derogations for specific situations (Article 49).

In Schrems II, the Court of Justice of the European Union annulled the adequacy decision previously in force in respect of the United States.¹⁶ In the absence of an adequacy decision since July 2020, transfers to the United States cannot be based on Article 45 of the GDPR.

Article 46(1) provides of the GDPR, *inter alia*, that in the absence of a decision in accordance with Article 45(3), a controller or processor may only transfer personal data to a third country after having taken appropriate safeguards, and subject to the

¹⁶ 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 Privacy Shield of the European Union and the United States and the judgment of the Court of Justice of the European Union Facebook Ireland and Schrems (Schrems II), C-311/18, EU:C:2020:559.

availability of statutory rights of data subjects and effective remedies for data subjects. Article 46(2)(c) provides that such appropriate safeguards may take the form of standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).

In Schrems II, the Court of Justice did not reject standard contractual clauses as a transfer tool. However, the Court found that they are not binding on the authorities of the third country. In that regard, the Court held that '*Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.*'¹⁷

The reason why the Court of Justice of the European Union annulled the adequacy decision with the US was how the U.S. intelligence agencies can access personal data. According to the Court of Justice, the conclusion of standard contractual clauses cannot in itself ensure a level of protection required by Article 44 of the GDPR, as the safeguards set out therein do not apply when such authorities request access. The Court of Justice of the European Union therefore stated:

*'It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection.'*¹⁸

The recommendations of the European Data Protection Board (EDPB) on the consequences of the judgment¹⁹ clarify that if the assessment of the law and practice of the third country means that the protection guaranteed by the transfer tool cannot be maintained in practice, the exporter must, in the context of his transfer, as a rule either suspend the transfer or take appropriate supplementary measures. In that regard, the EDPB notes that '*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it - by itself or in combination with others - addresses the specific deficiencies identified in your assessment of the situation in the third country as regards its laws and practices applicable to your transfer. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.*'²⁰

¹⁷ Points 125-126.

¹⁸ Paragraph 133.

¹⁹ 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 (hereinafter "EDPB Recommendations 01/2020").

²⁰ EDPB Recommendations 01/2020, item 75.

The recommendations of the EDPB show that such supplementary measures can be divided into three categories: contractual, organisational and technical.²¹

As regards *contractual* measures, the EDPB states that such measures "*In some situations, these measures may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country*" [...]. Provided the nature of contractual measures, generally not capable of binding the authorities of that third country when they are not party to the contract, these measures may often need to be combined with other technical and organisational measures to provide the level of data protection required [...]."²²

With regard to *organisational* measures, the EDPB stresses "[a] electing and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. Depending on the specific circumstances of the transfer and the assessment performed on the legislation of the third country, organisational measures are needed to complement contractual and/or technical measures, in order to ensure a level of protection of the personal data essentially equivalent to that guaranteed within the EEA".²³

With regard to *technical* measures, the EDPB points out that 'measures, which may supplement safeguards found in Article 46 GDPR transfer tools to ensure compliance with the level of protection required under EU law in the context of a transfer of personal data to a third country'.²⁴ The EDPB states in this regard that "The measures listed below are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. These measures would be necessary to guarantee an essentially equivalent level of protection to that guaranteed in the EEA, even if the public authorities' access complies with the law of the importer's country, where, in practice, such access goes beyond what is necessary and proportionate in a democratic society.⁷⁹ These measures aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other datasets that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts".²⁵

2.4.2 Assessment of the Swedish Authority for Privacy Protection (IMY)

2.4.2.1 Applicable transfer tool

The investigation shows that CDON and Google have entered into standard data protection clauses (standard contractual clauses) within the meaning of Article 46 for the transfer of personal data to the United States. These clauses are in line with those published by the European Commission in Decision 2010/87/EU and thus a transfer tool under Chapter V of the GDPR.

²¹ EDPB Recommendations 01/2020, item 52.

²² EDPB Recommendations 01/2020, item 99.

²³ EDPB Recommendations 01/2020, item 128.

²⁴ EDPB Recommendations 01/2020, item 77.

²⁵ EDPB Recommendations 01/2020, item 79.

2.4.2.2 Legislation and situation in the third country

As can be seen from the judgment in Schrems II, the use of standard contractual clauses may require supplementary measures. Therefore, an analysis of the legislation of the third country in question needs to be carried out.

IMY considers that the analysis already carried out by the Court of Justice of the European Union in Schrems II, which relates to similar circumstances, is relevant and topical, and that it can therefore serve as a basis for the assessment in the case without further analysis of the legal situation in the United States.

Google LLC, as an importer of the data to the United States, shall be classified as an electronic communications service provider within the meaning of 50 US Code § 1881(b)(4). Google is therefore subject to surveillance by U.S. intelligence agencies pursuant to 50 US § 1881a (“702 FISA”) and is therefore obliged to provide the U.S. government with personal data when 702 FISA is used.

In Schrems II, the Court of Justice of the European Union held that the US surveillance programmes based on 702 FISA, Executive Order 12333 (hereinafter ‘E.O. 12333’) and Presidential Policy Directive 28 (hereinafter ‘PPD-28’) do not meet the minimum requirements laid down in EU law in accordance with the principle of proportionality. This means that the monitoring programmes based on those provisions cannot be considered to be limited to what is strictly necessary. In addition, the Court found that the monitoring programmes do not confer rights on data subjects that may be invoked against US authorities in court, which means that those persons do not have the right to an effective remedy.²⁶

Against this background, IMY notes that the use of the European Commission’s standard contractual clauses is not in itself sufficient to achieve an acceptable level of protection for the transferred personal data.

2.4.2.3 Supplementary measures implemented by Google and CDON

The next question is whether CDON has put in place supplementary measures.

As the controller and exporter of the personal data, CDON is obliged to ensure compliance with the rules of the GDPR. This responsibility includes, *inter alia*, assessing, on a case-by-case basis, in the case of transfers of personal data to third countries, which supplementary measures are to be used and to what extent, including assessing whether the measures taken together by the recipient (Google) and the exporter (CDON) are sufficient to achieve an acceptable level of protection.

2.4.2.3.1 Google’s supplementary measures

Google LLC, as an importer of personal data, has taken contractual, organisational and technical measures to supplement the standard contractual clauses. In its opinion of 9 April 2021, Google stated that it had taken action.

The question is whether the supplementary measures taken by CDON and Google LLC are effective, in other words, hindering the ability of U.S. intelligence agencies to access the transferred personal data.

²⁶ Paragraphs 184 and 192. Paragraph 259 et seq.

As regards the *legal and organisational measures*, it can be noted that neither information to users of the Tool (such as CDON), the²⁷ publication of a transparency report or a publicly available “government enquiries policy” prevents or reduces the ability of U.S. intelligence services to access the personal data. In addition, it is not described what it means that Google LLC’s “scrupulous review” of any “legality” request from U.S. intelligence agencies. IMY notes that this does not affect the legality of such requests as, according to the CJEU, they are not compatible with the requirements of EU data protection rules.

As regards the *technical measures* taken, neither Google LLC nor CDON have clarified how the described measures — such as the protection of communications between Google services, the protection of data when transferring between data centres, the protection of communications between users and websites, or “physical security” — prevent or reduce the ability of U.S. intelligence services to access the data under the US regulatory framework.

With regard to the encryption technology used — for example, for so-called “data at rest” (“data at rest”) in data centers, which Google LLC mentions as a technical measure — Google LLC as an importer of personal data nevertheless has an obligation to grant access to or supply imported personal data held by Google LLC, including any encryption keys necessary to make the data understandable.²⁸ Thus, such a technical measure cannot be considered effective as long as Google LLC is able to access the personal data in plain language.

As regards Google LLC’s argument that ‘*to the extent that data for measurement in Google Analytics transmitted by website holders constitute personal data, they may be regarded as pseudonymised*’, it can be concluded that Universal Unique Identifiers (UUIDs) are not covered by the concept of pseudonymisation in Article 4(5) of the GDPR. Pseudonymisation can be a privacy-enhancing technology, but the unique identifiers, as described above, have the specific purpose of distinguishing users and not serving as protection. In addition, individual identification is made through what has been stated above about the ability to combine unique identifiers and other data (e.g. metadata from browsers or devices and the IP address) and the ability to link such information to a Google account for logged-in users.

In the case of Google’s “anonymisation of IP addresses” in the form of truncation²⁹, Google’s response does not indicate whether this action takes place prior to transmission, or whether the full IP address is transmitted to the United States and shortened only after transmission to the United States. From a technical point of view, it has therefore not been shown that there is no potential access to the entire IP address before the last octet is truncated.

Against this background, IMY concludes that the supplementary measures put in place by Google are not effective, as they do not prevent US intelligence services from accessing the personal data or rendering such access ineffective.

²⁷ Regardless of whether such a notification would even be permitted under U.S. law.

²⁸ See EDPB Recommendations 01/2020, paragraph 81.

²⁹ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

2.4.2.3.2 CDON's own supplementary measures

CDON has stated that it has taken supplementary measures in addition to the measures taken by Google. According to the CDON, these consist of activating the function of truncating³⁰ the last octet of the IP address before the data is transmitted to Google, which means that the last octet is masked.³¹

As stated above with regard to Google's actions, it is not apparent from Google's reply whether this action takes place prior to transmission or whether the full IP address is transmitted to the United States and truncated only after the transfer to the United States. Therefore, from a technical point of view, it has not been established that, after the transmission, there is no potential access to the entire IP address before the last octet is truncated.

Even if the truncation were to take place before the transfer, it is not a sufficient measure, as the truncated IP address can be linked to other data, as IMY stated above in section 2.2.2. A truncation of an IP address means that only the last octet is masked, which in itself can only be any of 256 options (i.e. in the range 0-255) and because the truncated IP address can be distinguished from other IP addresses, this data can be linked to other data (as described in section 2.2.2) and enable identification, which is sufficient in itself to determine whether the data is a personal data. Although the masking of the last octet constitutes a privacy-enhancing measure, as it limits the scope of the data that authorities can access (in third countries), IMY notes that it is nevertheless possible to link the transferred data to other data which are also transferred to Google LLC (in third countries).

Against this background, IMY also notes that the supplementary measures taken by CDON in addition to the supplementary measures taken by Google are not effective enough to prevent US intelligence services from accessing the personal data or rendering such access ineffective.

2.4.2.3.3 Conclusion of the Swedish Authority for Privacy Protection (IMY)

IMY finds that CDON and Google's actions are neither individually nor collectively effective enough to prevent U.S. intelligence services from accessing the personal data or rendering such access ineffective.

Against this background, IMY considers that neither standard contractual clauses nor the other measures relied on by CDON can support the transfer as set out in Chapter V of the GDPR.

With this transfer of data, CDON therefore undermines the level of protection of personal data for data subjects guaranteed by Article 44 of the GDPR.

IMY therefore concludes that CDON AB violates Article 44 of the GDPR.

³⁰ Truncation of IP address means that asterisks or zeros replace other digits in the last octets (last digits of an IP address, a number between 0 and 255).

³¹ See above in the section on CDON's submissions, under the heading 'Supplementary protective measures taken'.

3 Choice of intervention

3.1 Legal regulation

In case of breaches of the GDPR, IMY has a number of corrective powers available under Article 58(2)(a) to (j) of the GDPR, including reprimand, injunctions and administrative fines.

IMY shall impose fines in addition to or in place of other corrective measures referred to in Article 58(2), depending on the circumstances of each case.

Each supervisory authority shall ensure that the imposition of administrative fines on a case-by-case basis is effective, proportionate and dissuasive. This is set out in Article 83(1) of the GDPR.

Article 83(2) of the GDPR sets out the factors to be taken into account in determining whether an administrative fine is to be imposed, but also in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand under Article 58(2)(b) of the Regulation. Account must be taken of aggravating and mitigating circumstances in the case, such as the nature, gravity and duration of the infringement and the relevant past infringements.

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR, which aim to create a harmonised methodology and principles for the calculation of fines.³²

3.2 Should an administrative fine be imposed?

IMY has found above that the transfers of personal data to the United States carried out through the Google Analytics tool and for which CDON is responsible are contrary to Article 44 of the GDPR. Infringements of that provision may, in accordance with Article 83, impose fines.

Given, among other things, that CDON has transferred a large amount of personal data, that the processing has been going on for a long time and that the transfer has meant that the personal data could not be guaranteed the level of protection afforded in the EU/EEA, this is not a minor breach. A fine must therefore be imposed on CDON for the infringement found. See also below under 3.3 for a detailed description of the gravity of the infringement.

3.2.1 To what amount should the administrative fine be determined to?

In determining the maximum amount of a fine to be imposed on an undertaking, the definition of ‘undertaking’ used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR). It is clear from the Court’s case-law that this applies to any entity engaged in an economic activity, irrespective of its legal form and the way in which it is financed, and even if, in the legal sense, the entity consists of several natural or legal persons.³³

³² EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR.

³³ See judgment in Akzo Nobel, C-516/15, EU:C:2017:314, paragraph 48

Pursuant to Article 83(5)(c) GDPR, in the event of infringement of, inter alia, Article 44 in accordance with 83(2), administrative fines of up to EUR 20 million or, in the case of an undertaking, up to 4 % of the total global annual turnover in the preceding financial year, whichever is higher, are to be imposed.

IMY considers that the company's turnover to be used as a basis for calculating the administrative fine is CDON's annual report for 2022. The company had sales of approximately SEK 461 000 000 during that financial year. This amount is less than EUR 20 million and the administrative fine can therefore be set at an amount of up to EUR 20 million.

In determining the amount of the fine, IMY shall determine, having regard to the gravity of the infringement and taking into account both aggravating and mitigating factors, an administrative fine amount which is effective, proportionate and dissuasive in the individual case.

IMY considers that the following factors are relevant to the assessment of the gravity of the infringement.

As far as the assessment of the gravity of the infringement is concerned, there are, at the outset, factors that lead to a more serious assessment of the infringement. CDON is transferring a large amount of personal data to third countries. The transfer has meant that the personal data have not been guaranteed the level of protection afforded in the EU/EEA, which in itself is a serious breach. In addition, it is aggravating that the transfer of personal data has been going on for a long time, i.e. from 14 August 2020 and is still ongoing, and that it has taken place systematically. IMY also takes into account that it has now elapsed around 3 years since the Court of Justice of the European Union, by judgment of 16 July 2020, rejected the Commission's adequacy decision in the United States,³⁴ thereby changing the conditions for transfers of personal data to the United States.

In the meantime, the EDPB made recommendations on the consequences of the judgment that had been put out for public consultation on 10 November 2020 and adopted in final form on 18 June 2021. In addition, several other EU/EEA supervisory authorities have issued injunctions to discontinue the use of the Tool until sufficiently effective security measures have been taken by the controllers. The decisions have covered cases where the controllers have also taken measures such as the "anonymisation of IP addresses" in the form of truncation.³⁵

Although these recommendations and decisions clearly point to the risks and difficulties of ensuring an adequate level of protection for data transfers to U.S. companies, CDON has not put in place supplementary measures of its own. Google's³⁶ IP truncation action means that the IP address can still be distinguished as

³⁴ 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-US Privacy Shield.

³⁵ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

³⁶ Truncation of IP address "anonymisation of IP address" means that asterisks or zeros replace other digits in last octets (last digits of an IP address, a number between 0 and 255), which in itself can only be any of 256 options. The effect of this measure means that it is still possible to distinguish the IP address from the other IP addresses (255 options), as the IP address can be linked with other transmitted data (e.g. information about the entity and time of visit) to third countries (to the USA).

it can be linked to other data transmitted to third countries (to the United States). This enables identification, which means that the data together constitute personal data.

The CDON website is also a well-attended e-commerce portal that offers goods from many different suppliers and is available in several countries and in several languages. These are data on a large number of data subjects in the EU/EEA that can be identified indirectly and whose data can be linked to other data relating to them. As regards the nature of the data, it follows from CDON's own purpose of processing — i.e. to be able, *inter alia*, to draw conclusions on how data subjects navigate and find the Website, that the data taken together make it possible to draw relatively precise conclusions about the privacy of data subjects and to map them, such as what they buy and which goods they are interested in over time. CDON's analysis of the Tool shows that the company have a proposal for a solution other than the Tool, but the company has chosen not to introduce this solution due to the fact that such a change would be particularly burdensome for the company. CDON's processing of personal data entails obvious risks of serious violation of the rights and freedoms of individuals, which gives CDON a special responsibility which imposes high standards in the case of transfers to third countries, where IMY overall considers that CDON has not demonstrated that it has carried out sufficient analysis and mapping, nor has it taken the necessary security measures to limit the risks to the data subjects.

At the same time, IMY notes that there are factors that speak in the opposite direction. IMY takes into account the specific situation arising after the judgment and the interpretation of the EDPB's recommendations, where there has been a gap after the transfer tool to the United States has been rejected by the Court of Justice of the European Union, according to the Commission's previous decision. IMY also takes into account that CDON has taken some, albeit insufficient, measures to restrict the personal data transmitted by activating the "anonymisation of IP addresses" by truncation.³⁷ That fact is also taken into account when assessing the gravity of the infringement.

Overall, considering the facts set out in this decision, IMY considers that the infringements in question are of a low degree of seriousness. The starting point for calculating the fine should therefore be set low in relation to the maximum amount in question. In order to ensure a proportionate fine in the individual case, it is also necessary, at this stage, to further adjust the starting point for the further calculation downward, taking into account the high turnover underlying the calculation of the fine.

In addition to assessing the gravity of the infringement, IMY shall assess whether there are any aggravating or mitigating circumstances that have a bearing on the amount of the fine. IMY considers that there are no additional aggravating or mitigating circumstances, other than those taken into account when assessing the severity, which affect the amount of the fine.

On the basis of an overall assessment of the above facts and in the light of the fact that the administrative fine must be effective, proportionate and dissuasive, IMY considers that the fine may remain at SEK 300 000 (three hundred thousand).

³⁷ Decision of the Austrian Supervisory Authority (Datenschutzbehörde) of 22 April 2022 concerning complaints Google Analytics represented by NOYB with local case number 1354838270, the French Supervisory Authority (CNIL) decision of 10 February 2022 represented by NOYB and the Italian Supervisory Authority (Garante) decision of 9 June 2022 concerning complaints Google Analytics represented by NOYB, local case number 9782890.

3.3 Other interventions

Against this background IMY considers that CDON should be ordered pursuant to Article 58(2)(d) of the GDPR to ensure that its processing of personal data in the context of its use of the Google Analytics tool complies with Article 44 and the other provisions of Chapter V. In particular, by discontinuing the use of the version of the Google Analytics tool used on 14 August 2020, unless appropriate safeguards are in place. The measures shall be implemented no later than one month after the date of entry into force of this Decision.

4 How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection's contact details are set out in the first page of the decision.

This decision was taken by Director-General [REDACTED] following a presentation by the legal advisor [REDACTED]. [REDACTED], Head of Legal Affairs, [REDACTED], Head of Unit and information security specialist [REDACTED]. [REDACTED] have also participated in the final proceedings.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's draft decision in case with national reference number, DI-2019-11737. Only the Swedish version of the decision is deemed authentic

Registration number:
DI-2019-11737

Date:
2023-06-26

Decision under the General Data Protection Regulation –Bonnier News AB

Content

1. Decision of the Authority for Privacy Protection	3
2. Presentation of the supervisory case	3
2.1 Description of the group common processing of personal data	4
2.1.1 Description of the processing of personal data contained in the behavioural database	5
2.1.2 Description of the processing of personal data stored in KDB	6
3. Statement of reasons for the decision	8
3.1 IMY's competence	8
3.1.1 Circumstances at issue	8
3.1.2 Applicable provisions, etc	8
3.1.3 IMY assessment	9
3.2 Bonnier News AB's responsibility for the data processing	9
3.2.1 Circumstances at issue and Bonnier News AB's position	9
3.2.2 Applicable provisions, etc	9
3.2.3 IMY assessment	10
3.3 What constitutes personal data?	10
3.3.1 Circumstances at issue and Bonnier News AB's position	10
3.3.2 Applicable legal provisions other legal sources	11
3.3.3 IMY's position	12
3.4 The processing constitutes profiling	13
3.4.1 Applicable provisions	13
3.4.2 IMY's position	13
3.5 Legal basis for processing for the purpose of displaying personalised advertisements based on data in the behavioral database	13
3.5.1 Circumstances at issue and Bonnier News AB's position	13

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

3.5.2 Applicable provisions, etc.....	15
3.5.3 Basic principles for IMY's assessment.....	17
3.5.4 Legitimate interest.....	19
3.5.5 Is the processing necessary for the legitimate interest?	19
3.5.6 Balancing test test for the processing of personal data in supplemented behavioural profiles	19
3.5.7 Balance of interests for the processing of personal data in simple behavioural profiles	21
3.6 Legal basis for processing for the purpose of making contact information available for telemarketing and postal direct marketing.....	22
3.6.1 Applicable provisions, etc.....	22
3.6.2 Circumstances at issue and Bonnier News AB's position.....	22
3.6.3 IMY's assessment.....	24
3.6.4 Legitimate interest.....	24
3.6.5 Is the processing necessary for the legitimate interest?	24
3.6.6 Balance of interests for the processing of personal data in supplementary customer database profiles	24
3.6.7 Balance of interests for personal data not linked to the behavioural database	25
3.7 Choice of corrective measure	26
3.7.1 Applicable provisions etc.....	26
3.7.2 Same or interconnected data processing operations.....	26
3.7.3 Administrative fine.....	27

1. Decision of the Authority for Privacy Protection

The Swedish Authority for Privacy Protection notes that Bonnier News AB during the period from 7 November 2019 to 11 June 2020 has processed personal data without having a lawful basis pursuant to Article 6(1) of the GDPR¹ by:

- a) processing personal data for the purpose of profiling the data subjects based on their behavioural data in so-called supplemented behavioural profiles and making those profiles available to affiliated companies for the purpose of displaying targeted advertisements;
- b) processing personal data for the purpose of profiling the data subjects based on their behavioural data in so-called simple behavioural profiles and making those profiles available to affiliated companies for the purpose of displaying targeted advertisements;

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).

- c) processing personal data by profiling the data subjects based on their supplemented customer database profiles in order to make contact information available to affiliated companies for telemarketing and postal marketing;

Pursuant to Articles 58(2) and 83 of the GDPR, the Swedish Authority for Privacy Protection decides that Bonnier News AB shall pay an administrative fine of SEK 13 000 000 (thirteen million).

2. Presentation of the supervisory case

In a supervision of Bonnier Magazine and Brands AB (ref. DI-2019-6523), the Swedish Authority for Privacy Protection (IMY) has found that Bonnier News AB, together with other companies within the Bonnier Group, processes personal data for, amongst other, marketing purposes based on the lawful basis legitimate interest pursuant to Article 6(1)(f) of the GDPR. IMY has initiated supervision against Bonnier News AB in order to investigate whether Bonnier News AB complies with the GDPR requirements for the processing of personal data that takes place for marketing purposes.

Within the framework of the supervision, Bonnier News AB has been given the opportunity to give its opinion on seven complaints addressed to IMY concerning various marketing measures taken by companies within the Bonnier Group of companies.² According to Bonnier News AB those marketing actions mentioned in the complaints have not happened due to withdrawals from the group wide/group common databases. Bonnier News AB has therefore stated that they are not the controller for the processing of the complainants' personal data regarding marketing. In the light of the above, IMY does not find it appropriate to further investigate these complaints within the context/scope of this supervision/case.

Within the scope of the supervision, IMY has examined whether Bonnier News AB has a lawful basis pursuant to Article 6 of the GDPR for the processing of personal data in the group-wide/group common databases for marketing purposes. The supervision covers the processing of personal data conducted through creating profiles and making it available to affiliated companies to be used to display personalized advertisements. It also covers the processing of personal data, the creation of profiles and the making available of data to affiliated companies in order to be used by affiliated companies in telemarketing and postal direct marketing. IMY has not taken a position on whether Bonnier News AB's personal data processing otherwise complies with the General Data Protection Regulation.

The supervision was initiated with an inspection on 7 November 2019. In connection with IMY sending the inspection report to Bonnier News AB, IMY asked the company supplementary questions on 20 December 2019. Bonnier submitted its point of view on the inspection report and replied to IMY's questions on 14 February 2020. On 15 May 2020, IMY submitted further supplementary questions to Bonnier News AB, to which it replied on 11 June 2020. Due to Bonnier News AB's update of its personal data policy, the company submitted additional information on 21 July 2020.

Bonnier News AB has given its opinion on IMY's draft decision on 13 April 2023.

² DI-2018-22602, DI-2019-10121, DI-2019-10513, DI-2019-11057, DI-2019-7484, DI-2019-8104 and DI-2019-9556

As the case concerns cross-border processing, IMY has made use of the cooperation and consistency mechanisms provided for in Article 56 and Chapter VII of the GDPR. The concerned supervisory authorities have been the authorities of Denmark, Germany, Finland and Norway.

2.1 Description of the group common processing of personal data

The following circumstances have emerged during the inspection and subsequent exchange of documents. Within the Bonnier Group of companies there is a collaboration between Bonnier News AB and a number of affiliated companies that are part of the group of companies (the affiliated companies). Which companies are affiliated changes over time. At the time of the inspection, there were 15 affiliated companies, which decreased to 8 during the spring of 2020. The processing of personal data that takes place within the framework of the cooperation is limited to the affiliated companies customers on the Swedish market. The affiliated companies collect personal data from their customers and people who visit the company's websites. The data collected is transferred into two group common databases, one customer database (KDB) and one behavioural database (the behavioural database). These databases generate profiles of individuals. The profiles are also linked to information obtained from Bisnode Sverige AB.

Bonnier News AB has stated that it stores collected data in the group common databases in order to use for the following purposes:

- To establish a customer register for affiliated companies with good data quality, which includes compiling customer and user data and to verifying the accuracy, relevancy and appropriateness of the data
- To offer the customers of the affiliated companies an easy way to exercise their rights and an opportunity to ask questions about personal data to the joint customer service
- To make available personal data to affiliated companies in order to:
 - Use the contact details of other affiliated companies to enable marketing to the affiliated companies of its own products and services through postal direct marketing and telemarketing.
 - Display personalised content and ads in the affiliated companies digital services, based on customer and user's customer profile and behaviour on the affiliated companies sites.
 - Perform analysis of customer data to gain customer insight in order to conduct customer communications, marketing of its own products, services and customer service.
 - Perform analysis of customer data in order to improve and develop existing services and products.

The personal data processing that takes place for the purpose of adapting the advertisements of affiliated companies is based on data stored in the behavioural database. The personal data processing that takes place to disclose personal data to affiliated companies for use in telemarketing and postal direct marketing is based on data in KDB.

2.1.1 Description of the processing of personal data contained in the behavioural database

The inquiry in the case shows the following.

The data stored in the behavioural database is processed for the purpose of displaying personalised content and personalised advertisements in the digital services of the affiliated companies.

When an individual visits an affiliated company's website, the affiliated company collects information about the individual's browsing pattern. This is enabled through a script on the affiliated company's website requesting to save a text file (cookie) on the visitor's computer, tablet or mobile phone. The information contained in the cookie can be used to track the user's browsing pattern on the website. The data (behavioural data) collected when the individual browses and is then transferred to the behaviour database and added to the individual's profile is:

- Information on the URL (the visited webpage), its category and a content tag³.
- Information on the user's device in which the webpage view took place, the browser type and the part of the user's IP address identifying the country;
- Information on the behaviour in terms of the time spent on and time stamp for the page view;
- Information on a unique, randomly generated cookie value ('cookie identifier');
- Information on whether the page view took place in log-in mode.

Bonnier News AB erase the cookie identifier after 30 days and as of day 31, the generated behavioural data is no longer used for personalised advertisements to private individuals.

Data in the behavioural database and in KDB may in some cases be linked together.

Where the data in the behavioural database cannot be linked to KDB data, the behavioural profile of the data subject consists only of the data listed above, a profile which for the purposes of this decision will be referred to as "*simple behavioural profile*".

Where data in the behavioural database and data in KDB can be linked together in the behavioural database, data from KDB is added regarding the purchase history, gender, age, car ownership of the household and postal code, as well as statistical variables based on the private individual's residential area such as life phase, purchasing power and housing form to the behavioural database. For the purpose of this decision, these profiles will continue to be referred to as "*supplemented behavioural profile*".

The process of making data available to affiliated companies is done through a search tool that is linked to the behavioural database where the affiliated company can order a

³ A content tag is a description of the content that has been consumed in the services of the participating companies. Bonnier News AB collects two types of tags, predefined according to IAB's (The Interactive Advertising Bureau) standard and tags produced by the affiliated companies' editorial boards.

segment of customer data based on its chosen variables. An administrator will review whether the order meets the cooperation specific criteria. If this is the case, the affiliated company will gain access to a code that enables it to target ads at users included in the segment.

The affiliated companies can only retrieve data from the behavioural database based on behavioural data that has been collected from the company's own digital services. This applies regardless of whether it is a simple or supplementary behavioural profile. Regarding the supplemented behavioural profile however, it may contain purchase history from other affiliated companies as well. In KDB, data is erased after two years upon which data older than that cannot be linked to the behavioural database or disclosed to affiliated companies.

2.1.2 Description of the processing of personal data stored in KDB

The inquiry in the case shows the following.

The information about private individuals contained in KDB is processed for the purpose of being used by affiliated companies for the marketing of their own products and services through postal direct marketing and telemarketing.

In connection with an individual making a purchase or signing up to a subscription, the affiliated company that has a contractual relationship with the customer collects data from the customer. A portion of this data is transferred to KDB. In KDB, information is linked to a profile. In KDB, the customer profile is assigned a KDB ID. If the affiliated company's customer is already registered in KDB, the existing customer profile is updated/supplemented with the new engagement. In the absence of a pre-existing customer profile, a new customer profile is created with a new KDB ID. The data stored in KDB collected from the customer's contact with the affiliated company is the name, address, telephone number, national identification number national identification number, e-mail address and information related to the customer's purchase, such as product category, brand, type of packaging (whether it is a digital or traditional product and whether it is a free or paid product). It is also registered in the KDB if the customer has objected to its data in the KDB being used for marketing purposes and information whether the customer has registered in the so-called NIX register. There are limitations for the following categories of data:

- The e-mail address is not disclosed to affiliated companies for the purpose of telemarketing and postal direct marketing.
- The national identification number is only used to verify whether the customer has signed up to object to marketing measures in the NIX register (NIX-spärr) and to check that the customer is not deceased.
- The national identification number is not made available to the affiliated companies.

In addition to the data collected by the affiliated companies, Bonnier News AB collects data from Bisnode Sverige AB in order to control and supplement the contact details of individuals, as well as to provide statistical data such as life phase, purchasing power and form of housing. Furthermore, data on car ownership and deceased persons are collected as well as information on a so-called GEDI ID (which is a unique identifier in the form of a pseudonymized ID).

Data in KDB and the behavioural database may in some cases also be linked in KDB. The profile then constitutes what in this decision hereinafter will be referred to as *supplemented customer database profile*. This is done by a customer of an affiliated

company visiting the company's website and logging into his account. The behavioural data that has been collected regarding the customer and which is linked to a cookie identifier can under certain conditions be linked to the customer's KDB ID. In cases where the customer's KDB ID and the value of the cookie can be linked together, the KDB profile is supplemented with data collected in the last 30 days from the behavioural database. The data collected is information about which websites the customer has visited, which section of the website the customer visited (so-called content tags), and what device type the customer have used for browsing. Bonnier News AB has limited the type of content tags on which companies other than the one whose website the individual have accessed can base their profiling on for the purposes of telemarketing and postal direct marketing.⁴

When a person ceases to be a customer of an affiliated company, KDB is notified that the customer's engagement has ended and the customer is flagged as a passive customer. The customer's data will then be deleted in KDB after two years. Data collected from the behavioural database is deleted after 30 days. Any NIX blocking is always activated when making contact information in KDB available to other affiliated companies' customers and contact details of their own customers when they have been passive for 12 months.

The data is made available to affiliated companies upon request through an application in KDB. In KDB, a sample file is created based on the criteria specified by the affiliated company. Within the framework of the cooperation, something called purpose-adapted schemes is applied. These regulate what information is disclosed from KDB. At the point of disclosure, only the data points defined as necessary for the marketing channel indicated at the time of disclosure are provided, i.e. telephone numbers at a telemarketing campaign and addresses used for postal direct marketing. The data points on which the segmentation was based are not disclosed. The data is made available through an interface in KDB to the affiliated company.

It is possible for the data subject to request erasure from KDB. The data subject also has the right to object to the use of their data for telemarketing and postal direct marketing.

Bonnier News AB has stated that all affiliated companies are majority owned by Bonnier Group AB and are subject to the Bonnier Group's framework for processing personal data and that only a small part of the profiles in question could be linked to data in the behavioural database.

3. Statement of reasons for the decision

3.1 IMY's competence

3.1.1 Circumstances at issue

Part of the personal data processed within the group common cooperation has been collected through affiliated companies having placed a cookie on the visitor's computer, surf tablet or mobile phone. Bonnier News AB has stated that the collection is made through the websites of affiliated companies. The affiliated companies then transfer this data to the behavioural database and in some cases the data is also linked to profile information in KDB. Bonnier News AB has stated that the obligations arising from the provisions of the Electronic Communications Act (2003:389) and the

⁴ Only tags categorised with IAB's taxonomy are collected.

since adopted Electronic Communications Act (2022:482) on Electronic Communications (LEK), aimed at affiliated companies and not Bonnier News AB because it is the affiliated companies that are responsible for the processing that is the actual collection of the data.

3.1.2 Applicable provisions, etc.

Pursuant to Article 95 of the GDPR, the GDPR shall not impose any additional obligations on natural or legal persons that process personal data within fields that are already subject to obligations under the so-called ePrivacy directive⁵. The ePrivacy directive has been implemented in Swedish law through LEK, where, *inter alia*, the collection of data through cookies is regulated.

Pursuant to Chapter 9, Section 28 of the LEK, data may be stored in or gained from a subscriber's or user's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and has given his consent to it. Furthermore, it follows that this does not prevent the storage or access necessary to transmit an electronic message over an electronic communications network or which is necessary for the provision of a service expressly requested by the user or subscriber. Prior to August 1st 2022, when the LEK entered into force, corresponding requirements were made pursuant to Chapter 6, Section 18 of the Electronic Communications Act (2003:389). The Swedish Post and Telecom Agency (PTS) is the supervisory authority pursuant to the LEK (Chapter 1, Section 5 of Ordinance [2022:511] on electronic communications).

The EDPB has stated in its opinion on the interplay between the ePrivacy directive and the General Data Protection Regulation⁶. It follows, *inter alia*, that the national supervisory authority appointed under the ePrivacy directive is solely competent to oversee compliance with the directive. However, according to the GDPR, the supervisory authority is the competent supervisory authority for the processing which is not specifically regulated in the ePrivacy directive. If only part of the processing falls within the scope of the ePrivacy directive, this does not limit the supervisory authority's power to examine other parts of the processing pursuant to the GDPR.⁷

This means, *inter alia*, that the data protection authority under the GDPR is competent under the GDPR to assess the lawfulness of the processing of personal data that takes place after the data has been retrieved from the individual's terminal equipment, such as the storage of collected data and the analysis of data for purposes of online behavioural advertising.⁸

3.1.3 IMY assessment

The data supplied to the behavioural database has been collected by the affiliated companies through cookies. The processing of personal data that is under investigation in this supervisory case is Bonnier News AB's subsequent processing of personal data in the behavioural database. Said processing is not covered by the regulations in the LEK or the previously applicable regulation in the Electronic

⁵ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

⁶ Opinion 5/2019 on the interaction between the ePrivacy Directive and the general public General Data Protection Regulation, in particular as regards the competences, tasks and powers of data protection authorities, adopted on 12 March 2019

⁷ See paragraphs 68 and 69 of the opinion.

⁸ See paragraph 75 of the opinion.

Communications Act (2003:389). This means that the GDPR applies to the processing and that IMY is the competent supervisory authority.

3.2 Bonnier News AB's responsibility for the data processing

3.2.1 Circumstances at issue and Bonnier News AB's position

It is Bonnier News AB's position that Bonnier News AB and each affiliated company have a joint controllership and responsibility for the processing that takes place in KDB and the behavioural database for the purposes set out above as common. Furthermore, Bonnier News AB has stated that Bonnier News AB and its affiliated companies share a joint view of the purposes and means and that Bonnier News AB has entered into the Joint Data Controller Agreement with the affiliated companies pursuant to Article 26(2) of the GDPR.

Bonnier News AB has stated that each affiliated company has its own independent ("local") controller responsibility for its own collection of the data. Bonnier News AB has further stated that it has no joint controller responsibility for the personal data processing carried out at the point after which the data has been disclosed to affiliated companies from the group common databases. It is the affiliated company that retrieves the data that is responsible for the processing carried out by this company after collection.

3.2.2 Applicable provisions, etc.

Pursuant to Article 4(7) of the GDPR, the controller is the person who alone or jointly with others determines the purposes and means of the processing of personal data. The fact that the purpose and means can be determined by more than one actor means that several actors can be controllers for the same processing.

Pursuant to Article 4(2) of the GDPR, processing is a measure or combination of measures involving personal data or sets of personal data.

The Court of Justice of the European Union has held in the Fashion-ID judgement that a website owner who uses social network plug-ins on its website may become a joint controller with the social network. This applies to the processing of collection and disclosure by transmission of the personal data of website visitors using the social network plug-in. The Court also held that each party is responsible only for those parts of the processing chain for which it actually determined the purpose and means.⁹

In Wirtschaftsakademie, the Court of Justice held that joint controller responsibility for processing does not necessarily mean that the various actors involved in the processing of personal data have the same responsibility.¹⁰ On the contrary, those actors may be involved at different stages of the processing of personal data and to different degrees, for which each actor's level of responsibility must be assessed in the light of all the relevant circumstances of the individual case.

3.2.3 IMY assessment

Bonnier News AB provides two databases, the KDB and the behavioural database, from which data from affiliated companies are merged into profiles of private individuals. Subject to the conditions determined by Bonnier News AB and the

⁹ See judgment in Fashion-ID, C-40/17, EU:C:2019:629, paragraph 64-85

¹⁰ See judgment in Wirtschaftsakademie, C-210/16, EU:C:2018:388, paragraph 43

companies, the information is made available to Bonnier News AB and affiliated companies.

IMY notes that, in addition to making the databases available to the affiliated companies, Bonnier News AB has together with the companies decided the framework for the processing in various ways.

In light thereof, IMY makes the assessment that Bonnier News AB is joint controller of the data along with the affiliated companies for the part of the personal data processing that takes place for the common purposes of making personal data available, through profiling of private individuals' data, to affiliated companies to display personalised advertisements and for use in telemarketing and postal direct marketing. This includes the collection of data to the databases, the storage in the databases and the profiling, the collection of additional data from Bisnode Sverige AB, the interconnection that occurs between the behavioural database and KDB, and the transfer of data between the databases. Furthermore, Bonnier News AB is jointly responsible for personal data with the affiliated companies for the actions that take place before and upon a disclosure to an affiliated company.

3.3 What constitutes personal data?

3.3.1 Circumstances at issue and Bonnier News AB's position

Under the section titled "Description of the group common personal data processing" the processing is described as a variety of data collected from private individuals are processed in KDB and the common behavioural database. Bonnier News AB considers that what is referred to in this decision as supplemented behavioural profile constitutes personal data. However data in the behavioural database – which cannot be linked to data in KDB – constitute anonymous behavioural data according to Bonnier News AB. This is because they cannot be linked to a person either via KDB ID, customer ID, IP address or any other identifier of a person. Bonnier News AB therefore considers that the behavioural profiles referred to in this decision as simple behavioural profiles do not constitute personal data. The segmentation made on these simple profiles is, according to Bonnier News AB, only based on the affiliate's own collected information in the behavioural database (a company can, for example, choose to adapt sports-related content and advertisements to the data recorded via a cookie in the last 30 days).

3.3.2 Applicable legal provisions other legal sources

Pursuant to Article 4(1) GDPR, personal data is any information relating to an identified or identifiable natural person (i.e. the data subject). From the same provision, it follows that an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or online identifiers or one or more factors specific to the natural person's physical, physiological, genetic, mental, economic, cultural or social identity.

According to Recital 26 of the GDPR, the principles of data protection should apply to all information relating to an identified or identifiable natural person. Personal data which have undergone pseudonymisation which could be attributed to a natural person by the use of additional information should be considered as information on an identifiable natural person. In order to determine whether a natural person is identifiable, account should be taken of all means, such as singling out which, either by the controller or by another person, may reasonably be used to identify the natural person directly or indirectly. In order to determine whether means are reasonably likely

to be used to identify the natural person, account should be taken of all objective factors, such as the costs and duration of identification, taking into account both the available technology at the time of processing and technological developments. The principles of data protection according to recital 26 should not apply to anonymous information that does not relate to an identified or identifiable natural person, or to personal data rendered anonymized in such a way that the data subject is no longer identifiable. The Regulation therefore does not concern the processing of such anonymous information, which includes information for statistical or research purposes.

According to recital 30 of the GDPR, natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as IP addresses, cookie identifiers or other identifiers, such as radio frequency identifications tags. This may leave traces that, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of natural persons and identify them.

An opinion of the Article 29 Working Party,¹¹ which contains an analysis of the concept of personal data, shows that a natural person in a group is considered to be 'identified' when he or she can somehow be 'singled out' from other persons.¹² The European Data Protection Board (EDPB) has stated in its guidelines on targeting users through social media advertising that even persons who use a social media service without having created an account or profile with the social media service may constitute data subjects within the meaning of Article 4(1) of the GDPR if the person is directly or indirectly identified or identifiable.¹³ In that regard, the EDPB refers to the concept of 'singling out' in recital 26 of the GDPR and to the abovementioned opinion of the Article 29 Working Party.

The Article 29 Working Party's opinion on online behavioural based advertising further develops what it means to be identifiable:

The Article 29 Working Party states that behavioural based advertising often leads to the processing of personal data. Behavioural based advertising typically includes the collection of IP addresses and the processing of unique identifiers (through the web cookie). The use of such functions with a unique identifier makes it possible to track users of a particular computer even if dynamic IP addresses are used. In other words, such functions make it possible to "singled out" individual data subjects, even if their names are not known. In addition, the information collected in behavioural advertising relates to (i.e. is about) a person's characteristics or behaviour and is used to influence that particular person. This approach is further reinforced by taking into account the possibility that profiles can be linked at any time to directly identifiable information provided by the data subject, such as information provided when registering on a website. Other scenarios that may lead to identification include mergers, data losses and the growing availability of personal data linked to IP addresses on the Internet¹⁴

¹¹ The so-called Article 29 Working Party was an advisory and independent working group composed of representatives of the supervisory authorities of the EU and the EEA. The task of the group was to contribute, inter alia, to the uniform application of the Data Protection Directive through recommendations. The Working Party has been replaced on 25 May 2018 by the EDPB.

¹² See WP 136. Article 29 Working Party Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, p 12(f)

¹³ See EDPB Guidelines 8/2020 on Targeted Advertising in Social Media Version 2.0, adopted 13 April 2021, p 19

¹⁴ See WP 171, Opinion 2/2010 of the Article 29 Working Party on behavioural advertising on the Internet, adopted on 22 June 2010, p. 9(f)

3.3.3 IMY's position

IMY notes that the supplemented behavioural profiles (i.e. behavioural profiles linked to KDB) contain data relating to identified or identifiable natural persons. The supplementary behavioural profiles are therefore personal data.

With regard to the simple behavioural profiles (i.e. behavioural profiles not linked to KDB), IMY makes the following assessment.

In order for a data to be classified as personal data, it is necessary, first, that the data refers to a natural person. This requirement is met with regard to simple behavioural profiles because the data describe how the individual has surfed with a number of different parameters.

Furthermore, the natural person is required to be identified or identifiable. According to Article 4(1) of the GDPR, it is sufficient for a person to be identified indirectly for this requirement to be met. The provision further states that identification may be made by reference to an online identifier. Recital 30 of the Regulation lists cookies ("cookie identifiers" in the English language version) as an example of online identifiers. Identification within the meaning of Article 4(1) may therefore be carried out by means of unique web cookie values used in the behavioural database.

IMY further notes that from recital 26 of the GDPR it becomes apparent that singling out is a means of identifying a natural person. This means that one person can be identified by being distinguished from other persons.¹⁵ Thus, it is not required that the person be identified by name or national identification number. Such separation or screening occurs when the information being processed makes it possible to identify, draw conclusions or take specific action in relation to a user. In the behavioural database, the information is linked to a unique identifier, a unique cookie value, which is linked to a specific browser or app, which in turn is connected to a device such as a computer or phone. One of the purposes of the processing of the data is to target users through marketing based on the users previous behaviour in an identified browser or app on the basis of the user's behaviour. The purpose of the processing is thus to draw conclusions about the individual by creating a profile and based on this affect the individual. Thus, IMY notes that even the simple behavioural profiles not linked to KDB mean that individuals are identifiable.

Against this background, IMY considers that the simple behavioural profiles constitute personal data.

3.4 The processing constitutes profiling

3.4.1 Applicable provisions

Profiling is defined in Article 4(4) of the GDPR as any form of automated processing of personal data that consists of the use of personal data to assess certain personal characteristics of a natural person, in particular to analyse or predict that natural person's performance at work, financial situation, health, personal preferences, interests, reliability, behaviour, location or movements.

¹⁵ See WP 136.f Opinion 4/2007 of the Article 29 Working Party on the concept of personal data, adopted on 20 June 2007 p. 12

3.4.2 IMY's position

IMY notes that the processing, both of personal data based on simple behavioural profiles and supplemented behavioural profiles that take place for the purpose of making the data available to affiliated companies for the purpose of displaying personalised advertisements includes profiling of data subjects as defined in Article 4(4) of the GDPR. This is because it concerns the automatic processing of personal data aimed at categorising the data subjects according to their previous behavioural patterns, which in turn makes it possible to assess some of their personal characteristics.

IMY further notes that the processing of personal data for the purpose of making available contact details for telemarketing and postal direct marketing includes profiling of data subjects as defined in Article 4(4) of the GDPR. This is because it involves automated processing of personal data for the purpose of categorising data subjects based on their purchase history and, in some cases, also behavioural patterns.

3.5 Legal basis for processing for the purpose of displaying personalised advertisements based on data in the behavioral database

3.5.1 Circumstances at issue and Bonnier News AB's position

Bonnier News AB has stated that the activities within the Group has been coordinated in order to achieve a better data collection and make it possible to process the customers' and users' personal data for specified purposes in a cost-effective and integrity-friendly manner. Bonnier News AB uses profiling of private individuals to make data available to its affiliated companies for the purpose of displaying personalised advertisements, on collected behavioural data that cannot be linked to KDB, and on behavioural data which can be connected to the KDB and where additional personal data is added to the data subject's profile. Bonnier News AB relies on the legal basis of Article 6(1)(f) of the GDPR for this processing of personal data.

Legitimate interest

Bonnier News AB has stated the following.

The Company has a legitimate interest which consists in a need to understand its customers and users wishes and needs in order to achieve relevance in content and advertising targeted at customers and users and through it be able to offer competitive products/services and attractive advertising spaces. Many of the affiliated companies also engage in journalistic operations. Today, publishers' business model consists of revenue streams from reader and advertising income. The group common personal data processing is important for the financing of the companies' journalistic operations. Bonnier News AB has also pointed out the protection of freedom and diversity of the media in Article 11 of the EU Charter of Fundamental Rights.

Necessary processing

Bonnier News AB has stated that the processing of personal data is necessary in order to achieve the purposes of making available private individuals' profiles to affiliated companies in order to display personalised advertisements. The company, along with the other companies, has taken steps to minimise the number of data collected as well as to limit the duration of the processing of the data and to ensure that the databases are kept separate and that only certain data are transferred between them.

Balancing of interests

Bonnier News AB has stated the following.

Bonnier News AB's interest overrides the private individual's interest in the protection of their personal data.

The processing of personal data in order to display personalised advertisements based on the private individual's profile is an essential condition for journalists and publishers to earn revenue and by extension be able to conduct journalism.

There is a possibility to object to the profiling that is based on behavioral data. According to the information that private individuals receive in Bonnier News AB's personal data policy, the private individual can object to information about their online behaviour being processed in the group common customer database.¹⁶ The result is that the connection between the private individual's customer data and their browsing behaviour is removed.

The data subjects have a direct relationship with one or more affiliated companies. Users/customers have either visited an affiliated company's website, purchased products from an affiliated company or have an active digital subscription. Many of the customers are subscribers who have a long-term relationship with the company providing the service or product and can therefore be considered to reasonably expect that their data will be processed. Many readers have a strong commitment to their preferred type of news media. Customer profiles in KDB contains, to some extent, to unit-purchases such as literature, newspaper and goods. In these cases, the relationship between customer and supplier may be considered somewhat less unique. Furthermore, the interaction is voluntary, clear information is provided and there are alternative products such as printed newspapers that private individuals can view completely anonymously.

It is unlikely that the processing will have a negative impact on the data subject's interest. Private individuals' interaction with affiliated companies is voluntary and it is in their interest that the companies' services are as relevant as possible. Furthermore, Bonnier News AB has referred to the fact that the Article 29 working party has stated that targeted marketing based on simple customer profiles, such as gender, age, place of residence and general interests (e.g. "fashion") typically has no significant impact on private individuals. Furthermore, Bonnier News AB has taken steps to ensure that a minimum of data is processed in relation to the purposes as well as to reduce privacy risks in other respects. Among other things, the personal data is not shared with companies other than the affiliated companies within the group and all of these companies are subject to the Bonnier Group's framework for processing of personal data.¹⁷

The processing at issue falls within the data subject's reasonable expectations because the private individuals who come into contact with the companies do so out of their own free will in order to access content on websites, purchase services and/or products and that they always have a customer/user relationship with one or more companies within the group. The companies' privacy policies contain easy to understand information about how the processing of customers' and users' personal

¹⁶ The version of Bonnier News AB's personal data policy filed on 21 July 2020, see under the heading "How to access and control your personal data", file annex 20.1.

¹⁷ Further measures taken are set out in the opinion submitted on 14 February 2020 Annex 13, Annex O

data is conducted within the group. The processing carried out within the scope of the KDB and the behavioural database is closely related to the companies' services and products, which should indicate what the consumers can expect. The fact that many of the companies' products and services are provided online and, in many cases, free or funded through advertising should lead to a certain expectation and acceptance of certain personal data processing for, inter alia, the adaptation of content and advertising. Today, many digital products that are consumed by a very large proportion of consumers in society are adapted to the individual and it is Bonnier News AB's point of view that today's consumers expect that the digital products and services they consume to some extent will be adapted to the private individual.

3.5.2 Applicable provisions, etc.

Personal data shall be processed in a lawful, fair and transparent manner in relation to the data subject, pursuant to Article 5(1)(a) GDPR. The lawful processing of the data means, inter alia, that at minimum one of the conditions set out in Article 6(1) is fulfilled.

Consent pursuant to Article 6(1)(a), is one of the legal bases a controller can rely upon for the processing of personal data. Another legal basis pursuant to Article 6(1)(f) is legitimate interest, which requires that the following three cumulative conditions are met. There must be (i) a legitimate interest of the controller or of the third party to whom the data is disclosed, (ii) the processing of personal data must be necessary for the legitimate interest pursued by the controller and (iii) the data subject's interest in the protection of his or her personal data must not outweigh the interest of the controller.¹⁸

According to recital 47 of the GDPR, a legitimate interest may exist, for instance, where there is a relevant and appropriate relationship between the data subject and the controller, for example if the data subject is a customer of the controller. It is stated that the processing of personal data for direct marketing purposes may be regarded as a legitimate interest. Furthermore, it is stated that a legitimate interest requires a careful pre-assessment, including if the data subject can reasonably expect, at the time and in connection with the collection of personal data, that processing for the specified purpose may take place. The interests and fundamental rights of the data subject could, in particular, triumph that of the controller if personal data are processed in circumstances where the data subject cannot reasonably expect any further processing.

Pursuant to Chapter 9, Section 28 of the LEK, which implements Article 5(3) of the ePrivacy Directive in Swedish law, data may be stored in or retrieved from the user's or subscriber's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and consents to it. This does not prevent the storage or access necessary to transmit an electronic message over an electronic communications network or that is necessary to provide a service explicitly requested by the user or subscriber. Similar requirements previously applied in accordance with Chapter 6, Section 18 of the Electronic Communications Act (2003:389).

The EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications show that data collected on the basis of consent pursuant to Article 5(3) of the ePrivacy Directive or subject to the exceptions

¹⁸ See, Fashion ID, C-40/17, EU:C:2019:629, paragraph. 95.

in Article 5(3) of that Directive can only be further processed for another purpose, if the controller requests further consent or is supported by Union or Member State law.¹⁹ The EDPB further states that such further processing cannot be based on a compatibility test pursuant to Article 6(4) GDPR, as it would undermine the protection of the ePrivacy Directive. Furthermore, the EDPB states that consent must, when required by the ePrivacy Directive, be specific and informed, meaning that data subjects must be made aware of each one of the purposes for processing and have the right to refuse such specific purposes. Should further processing on the basis of a compatibility test under Article 6(4) GDPR be possible, the very principle of consent requirements of the current Directive would be circumvented²⁰

In the EDPB Guidelines on the targeting of social media users, personal data are divided into categories of data that the data subject actively and knowingly has provided to the controller, observed data provided by the data subject through his or her use of the service or entity and derived and inferred data created on the basis of the data provided by the data subject.²¹ According to the EDPB, there are two lawful bases that could be considered for processing such data that the data subject has actively and knowingly provided, those being consent under 6.1(a) and legitimate interest under 6.1 f GDPR. Regarding data collected through observed data provided by the data subject through the use of a service or entity, including data collected through cookies, the EDPB states that Article 6(1)(f) cannot provide a lawful basis for targeted advertising where private individuals are tracked across websites and locations.²² Furthermore, the EDPB states that for such processing, consent is probably the most appropriate lawful basis in Article 6 GDPR. The assessment should also consider the fact that the processing includes activities that the EU legislator has opted to provide additional protective measures.²³

In its guidelines on consent under Regulation 2016/679, the EDPB has stated that if controllers choose to rely on consent as lawful basis for any part of the processing, they must be prepared to respect this choice and stop this part of the processing if a private individual withdraws their consent. Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals. In other words, the controller cannot swap from consent to other lawful bases. The EDPB further states that, for instance, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent. Because of the requirement to disclose the lawful basis, which the controller is relying upon at the time of collection of personal data, controllers must have decided in advance of collection what the applicable lawful basis is.²⁴

According to an opinion of the Article 29 Working Party on the notion of the controller's legitimate interest in Directive 95/46/EC, when carrying out the balancing of interests test, account should be taken of the nature of the controller's legitimate interest, the damage to the controller if the data were to not be processed, the nature of the data, the way data are being processed, the status of the data controller and data subjects., the reasonable expectations of the data subjects as to what will happen to

¹⁹ See Guidelines 01/2020 on the processing of personal data in connection with connected vehicles and mobility-related applications, Version 2.0, Adopted on 9 March 2021, para. 53

²⁰ See previous note

²¹ See EDPB Guidelines 8/2020 on Targeted Advertising in Social Media Version 2.0, adopted 13 April 2021, para. 40

²² See previous note, paragraph 77

²³ See previous note paragraph 78

²⁴ See EDPB Guidelines 05/2020 on consent under Regulation (EU) 2016/679, Version 1.1, adopted on 4 May 2020, paras 122-123

their data and the consequences for the data subjects. If, after analyzing the above factors, the outcome of the balancing of interests' test is still unclear, the design of so-called additional safeguards may be decisive for the outcome of the balancing of interests' test.²⁵

The Article 29 Working Party guidelines on automated individual decision-making and profiling, provide guidance when profiling can be based on legitimate interests under 6.1(f). According to the Guidelines, the following elements are relevant:

- The level of detail in the profile.
- The comprehensiveness of the profile.
- The impact of the profiling.
- The safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.

In several opinions, the Article 29 Working Party has repeated its position that it is difficult to rely on Article 6(1)(f) GDPR for profiling that takes place for marketing or advertising purposes when private individuals are tracked across multiple websites, locations, entities, services or for data brokerage activities.²⁶

3.5.3 Basic principles for IMY's assessment

Bonnier News AB processes personal data for the purpose of making individuals' profiles available to affiliated companies in order to display personalised advertisements based on the lawful basis legitimate interest pursuant to Article 6(1)(f) of the GDPR. Before IMY examines whether the lawful basis may constitute the basis for Bonnier News AB's processing, IMY finds reason to consider how the processing relates to certain statements made in the EDPB guidelines.

According to the EDPB's guidelines on the targeting of social media users, regarding data that the data subject has actively and knowingly provided, both consent and legitimate interest may constitute a lawful basis for the processing. However, the guidelines show that for data collected through observation (e.g. through cookies), legitimate interest cannot serve as an appropriate lawful basis when targeted advertising is based on tracking individuals across websites and locations.

IMY points out that Bonnier News AB collects data for its behavioral database from several different websites, but an affiliated company can only retrieve data based on behavioural data collected from the company's own digital services. This applies regardless of whether it is a simple or supplementary behavioral profile.

The EDPB Guidelines on processing personal data in the context of connected vehicles and mobility related applications state that data collected on the basis of consent pursuant to 5.3 of the ePrivacy Directive can be further processed for another purpose only if the controller requests further consent or the processing is supported by EU or national law. The EDPB guidelines on consent in its section on interplay between consent and other lawful bases in Article 6 also addresses the situation when

²⁵ See Article 29 Working Party Opinion 6/2014 on the notion of the controller's legitimate interests in Article 7 of Directive 95/46/EC

²⁶ See the Opinion of the Article 29 Working Party on Automated Individual Decision-Making and Profiling under Regulation (EU) 2016/679, adopted on 3 October 2017, p. 15 and Opinion 6/2014 of the Article 29 Working Party on the concept of the controller's legitimate interest in Article 7 of Directive 95/46/EC, adopted on 9 April 2014, p. 47, and the examples of pp. 59-60 and EDPB Guidelines 8/2020 on targeted advertising in social media Version 2.0, adopted on 13 April 2021 p. 77

the data subject is informed that data will be processed on the basis of consent, while actually some other lawful basis is relied on, is fundamentally unfair to individuals.

IMY notes that the situation in the supervisory case differs to some extent from that described in these guidelines. In the supervisory case, it is the affiliated companies that collect the data in pursuant to 5.3 of the ePrivacy Directive and are therefore subject to the requirement of consent in said provision. The affiliated companies have to ensure that they have legal support for their processing under the ePrivacy Directive and the General Data Protection Regulation. The processing of personal data by the affiliated companies is not covered by this supervision.

It is not Bonnier News AB that collects the data on the basis of consent under the national provisions implementing Article 5(3) of the ePrivacy Directive. It is only when the affiliated companies enter the personal data into the behavioral database and KDB that Bonnier News AB's processing begins. Bonnier News AB therefore does not change lawful basis from consent to legitimate interest.

At the same time, IMY points out that Bonnier News AB is part of the same Group of companies as the affiliated companies and that Bonnier News AB is a joint controller with the affiliated companies for the processing of personal data in the databases. The establishment of group common databases should not mean that data subjects receive a lower level of protection than if the processing took place only at the group company that collected the personal data. In other words, Bonnier News AB should not have greater opportunities to process personal data on the lawful basis of legitimate interest than that of the affiliated companies. Therefore, according to IMY, the guidelines set out above should have an impact on the assessment of the possibility of using legitimate interest as a lawful basis in the supervisory case.

It can be inferred from the above stated that, pursuant to Article 6(1)(f) of the GDPR, the scope for further processing of data collected on the basis of consent under the LEK is very limited. At the same time, the GDPR does not prohibit the use of Article 6(1)(f) as the lawful basis for the type of processing in question. IMY therefore proceeds and examines whether the processing is based on Article 6(1)(f) of the GDPR. IMY's assessment of whether Bonnier News AB can rely its processing on Article 6(1)(f) of the GDPR is based on the three conditions that must be fulfilled under the provision:

- (i) Is there a legitimate interest of the controller or of the third party to whom the data are disclosed?
- (ii) Is the processing of personal data necessary for the legitimate interest pursued?
- (iii) Does the data subject's interest in protecting his or her personal data outweigh the controllers?

IMY deals with the first two steps of the balancing of interests test jointly for the supplemented and simple behavioural profiles (sections 3.5.3 and 3.5.4). The third and final steps are then dealt with separately for the supplemented behavioural profiles (section 3.5.5) and the simple behavioural profiles (section 3.5.6).

3.5.4 Legitimate interest

There is a commercial aspect to Bonnier News AB's interest in creating profiles to make data available to affiliated companies in order to display personalised ads. The commercial aspect of an interest does not preclude that the interest is justified, but determines whether that interest is lawful, specific and represent a real and present interest.²⁷

Bonnier News AB's and affiliated companies' interest is lawful, real and present. IMY therefore notes that Bonnier News AB's interest in creating profiles for making available as well as the affiliates' interest in processing personal data in order to display personalised advertisements based on customer and user customer profiles and behavioural profiles is legitimate.

3.5.5 Is the processing necessary for the legitimate interest?

The necessity requirement laid down in Article 6(1)(f) of the GDPR must be examined in conjunction with the principle of data minimisation set out in Article 5(1)(c).²⁸ The purpose of the processing is to make data available to affiliated companies in order to display personalised advertisements based on private individual profiles. The supervisory case has shown that Bonnier News AB, together with the affiliated companies, has taken steps to minimise the number of data collected and limit how long this data is processed, as well as to ensure that the databases in which the data are processed are kept separate and that only certain data are transferred in between the two databases. In light thereof, IMY considers that the processing described in this Decision is necessary for the stated purpose.

3.5.6 Balancing test for the processing of personal data in supplemented behavioural profiles

Bonnier News AB's interest in creating profiles to make data available to affiliated companies in order to display personalised advertisements can, according to the company, benefit the private individual either through higher revenues allowing for free or cheaper services or that the individual is provided with offers that they are interested in. Bonnier News AB has also emphasised that many of the affiliated companies are engaged in journalistic operations and that publishers' operating model of today consists of income streams from reader and advertising revenue and that the group common processing is important for the financing of the companies' journalistic operations. In those circumstances, the company considers that its interest is particularly important.

As IMY has already stated, the interest in displaying personalised advertisements is justified pursuant to and within the meaning of Article 6(1)(f) GDPR. On the question of the significance of this interest, IMY points out that the interest is not in itself journalistic, but of a commercial nature. Through profiling, knowledge about customers and potential customers is achieved, which enable revenue from personalised advertising. IMY considers that Bonnier News AB's and its affiliated companies' commercial interest does not weigh as heavily as Bonnier News AB claims.

As regards the assessment of the interests of data subjects, IMY considers the following.

²⁷ See Article 29 Working Party Opinion 6/2014 on the notion of the controller's legitimate interests in Article 7 of Directive 95/46/EC

²⁸ See judgment in Asociația de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064, paragraph 48

As pointed out above, Bonnier News AB collects personal data in the behavioural database that was originally collected by the affiliated companies through cookies. The consent requirement under Chapter 9, Section 28 of the LEK for the collection provides a high level of privacy protection and a possibility for data subjects to control the use of the collected data.²⁹ This protection, as stated by the EDPB in several of its guidelines, risks being undermined if the personal data collected are processed on the basis of other lawful bases, such as legitimate interest pursuant to Article 6(1)(f) GDPR. As IMY already has stated, Bonnier News AB should not have more possibilities than the affiliated companies to use the lawful basis, legitimate interest, for processing the personal data, than the affiliated companies which collect them by cookies. IMY therefore considers that the nature of the data implies that the interest of the data subjects should be given great weight in the balancing of interests test.

Furthermore, IMY considers that the possibility for using Article 6(1)(f) GDPR as the lawful basis for profiling based on observed data is limited (see EDPB Guidelines 8/2020 on targeted social media advertising p. 77-78). IMY notes that the nature of the processing also means that the privacy interest of the data subjects weighs heavily.

Bonnier News AB has pointed out that profiling and personalised advertisements can benefit the data subject by enabling higher revenues for the affiliated companies, which in turn enables them to offer free or cheaper services. It can also benefit the data subject by providing them with offers that they are interested in. IMY does not question that the processing may partly benefit the data subjects, but believes that the overall interest in profiling is to create advertising that is as accurate as possible in order to get customers and potential customers to buy goods or services and to receive revenue from such advertising.

In cases where behavioral data can be linked to KDB for the purpose of displaying personalised ads (the so-called “supplementary behavioral profiles”), IMY considers the following in its assessment. While data for profiling are not collected from different websites, which, according to the EDPB guidelines, would render the lawful basis in Article 6(1)(f) GDPR as appropriate, the profiling includes data collected from other contexts such as previous purchases, collected demographic data and statistical data. IMY considers that profiling is extensive in its nature and that such profiling is not something a data subject can expect without having consented to such processing of personal data.

In conclusion, IMY considers that the data subject's privacy interest outweighs the interests of Bonnier News AB and its affiliated companies.

In light thereof, IMY concludes that Bonnier News AB has processed personal data in breach of Article 6(1) GDPR in order to profile the data subjects based on their behavioural data in a so-called supplemented behavioural profile and make the profiles available to affiliated companies in order to display personalised advertisements.

3.5.7 Balance of interests for the processing of personal data in simple behavioural profiles

As IMY previously stated in section 3.5.5, Bonnier News AB's interest to create profiles to make data available to affiliated companies to show personalised ads is a commercial interest that does not weigh as heavily as Bonnier News AB claims.

²⁹ The same requirements under Chapter 6, Section 18 of the Electronic Communications Act (2003:389) applied at the time in the case.

Regarding the assessment of the interests of data subjects, IMY takes into account the following.

Bonnier News AB has taken measures to minimise the number of data collected, implemented privacy-enhancing rules in segmentation, introduced rules of deletion and ensured that data collected from an affiliated company can only be used by that company. Thus, profiling takes place only on a company's "own visitors".

Furthermore, Bonnier News AB, through its integrity policy, informs about the processing.

What has been stated above must be weighted against the fact that the collection and profiling of simple behavioural profiles allows for the mapping of individuals through observed data that entails a greater infringement of privacy than when the data were collected through the involvement of the data subject. IMY considers that the privacy interest of data subjects is of great significance due to the nature of the data (the fact that special protection in LEK is given to the collection of the data). As IMY has already stated, Bonnier News AB should not have greater possibility than the affiliated companies to base their processing on legitimate interest than the affiliated companies which collected the personal data using cookies. Furthermore, IMY believes that when private individuals surfing behaviour is monitored to display personalised advertising, this can give the data subject the feeling of loss of control over their data and the feeling of being monitored. This may result in private individuals being affected in the choice of what they see on a website.

In conclusion, IMY considers because the processing enables profiling of individuals, that the data subject's privacy interest outweighs the interests of Bonnier News AB and affiliated companies when processing personal data in simple behavioural profiles

In light thereof, IMY notes that Bonnier News AB has processed personal data without having a lawful basis pursuant to Article 6(1) GDPR in order to profile the data subjects based on their behavioural data in so-called simple behavioural profiles and make the profiles available to affiliated companies for the purpose of displaying personalised advertisements.

3.6 Legal basis for processing for the purpose of making contact information available for telemarketing and postal direct marketing

3.6.1 Applicable provisions, etc.

In order to be able to rely on Article 6(1)(f) GDPR, as explained above, the three conditions set out in the article must be fulfilled. There must be a legitimate interest of the controller or of the third party to whom the data are disclosed, the processing of personal data must be necessary for the legitimate interest pursued and the interest of the data subject in the protection of his or her personal data must not prevail that of the controller.³⁰

The Guidelines of the Article 29 Working Party and the EDPB on profiling and the application of Article 6 have been set out in Section 3.5.

³⁰ Judgment of the Court of Justice of the European Union Fashion ID, C-40/17, EU:C:2019:629, para. 95.

3.6.2 Circumstances at issue and Bonnier News AB's position

Bonnier News AB has stated that it has coordinated its activities in order to achieve a better data base and enable the personal data of customers and users to be processed for specified purposes in a cost-effective and privacy-friendly manner. Bonnier News AB creates profiles on individuals in order to make contact information available for telemarketing and postal direct marketing. The profiling that this entails is partly based on data in KDB collected from affiliated companies during purchases and subscriptions (so-called customer engagements), and partly on data collected from Bisnode Sverige AB and, for a small part of the profiles, data from the behavioural database. Bonnier News AB relies its processing on Article 6(1)(f) GDPR.

Legitimate interest

Bonnier News AB has stated that the affiliated companies have a legitimate interest in marketing their products and services in an efficient and privacy-friendly way.

Necessary treatment

Bonnier News AB has stated that they together with the affiliated companies have taken steps to minimise the number of data collected, how long data is being processed and, in order to comply with the data minimisation principle, kept the databases separated and only transferred certain data. Furthermore, Bonnier News AB has taken steps to ensure that no more information than is needed is disclosed to the affiliated companies. At the time of disclosure, only the data points defined as necessary for the marketing channel indicated at the time of disclosure are provided, i.e. telephone numbers in a telemarketing campaigns and postal direct marketing address. The data points on which segmentation was based are not disclosed.

Balancing of interests test

Bonnier News AB has stated the following.

Bonnier News AB's interest in making data available to affiliated companies based on the data subject's profile for the purpose of telemarketing and postal direct marketing outweighs the data subject's privacy interest.

By using the Group's existing resources for telemarketing and postal direct marketing, rather than buying the same information/resource from an external party, a cost saving is generated while allowing for a more controlled utilisation rate of addresses and phone numbers than would have been possible otherwise. The processing is also intended to save purchase costs.

Bonnier News AB, together with the affiliated companies, has taken steps to minimise the number of data collected, limit how long data is processed and in order to comply with the data minimisation principle, keep the databases separate. For the purposes of telemarketing and postal direct marketing, Bonnier News AB has limited the type of content tags generated by the data subject browsing on other companies' websites.³¹ Furthermore, a link between the databases could only be made with a small percentage of users.

³¹ Only tags categorised with IAB's taxonomy are collected.

Furthermore, within the framework of the cooperation, what is known as purpose-adapted schemes is applied. These regulate what information is disclosed from KDB. At the time of disclosure, only the data points defined as necessary for the marketing channel indicated at the time of disclosure are provided, such as telephone numbers in a telephone sales campaign and postal direct marketing address. The data points on which segmentation was based are not disclosed.

There is a possibility for the data subject to request deletion from the group common database. The data subject also has the right to object to the data being used for telemarketing and postal direct marketing.

The data subjects have a direct relationship with one or more affiliated companies. Users/customers have either visited an affiliated company's website, purchased products from an affiliated company or have an active digital subscription. Many of the customers are subscribers who have a long-term relationship with the company providing the service or product, and can therefore be considered to have a greater expectation that their data will be processed. Many readers have a strong commitment to their preferred type of news media. To some extent, customer profiles in KDB belong to unit-purchases such as literature, newspaper and goods purchases, where the relationship between customer and supplier may be considered somewhat less unique. Furthermore, the interaction is voluntary, clear information is provided and there are alternative products such as physical newspapers that private individuals can view completely anonymously.

According to Bonnier News AB, the processing is unlikely to have a negative impact on the data subject's interest.

The processing that takes place lies within the data subject's reasonable expectations because the individuals who come into contact with the companies do so out of free will in order to access content on websites, purchase services and/or products and the fact that they always have a customer/user relationship with one or more of the companies within the Group. Furthermore, the companies' integrity policy contains clear information about how customers' and users' personal data are processed and shared within the Group. The processing carried out within the framework of the KDB/behavioural database is closely associated with the companies' services and products, which should have an impact on the consumer's expectations. The fact that a group coordinates systems and central functions and, as a consequence, shares certain data for reasons of efficiency should not be unexpected for data subjects. Customers who have not signed up to the NIX register have a reasonable expectation that their contact details may be used for postal direct marketing or telemarketing. Consumers are accustomed to this type of marketing.

The Group common policy provides information about direct marketing and telemarketing. It shows that addresses and telephone numbers can be used by the Bonnier companies for direct marketing via mail and telephone sales through tele marketing. It also appears that the Bonnier companies can choose segments that they believe are relevant to the campaign in question, e.g. 'men in the age range 40-45 years living in the Stockholm area'. It also shows that Bonnier companies always respect NIX-blocks and whether someone has objected to the marketing.

3.6.3 IMY's assessment

IMY deals with the first two steps in the balancing of interests test jointly for the supplemented and simple behavioural profiles (sections 3.6.4 and 3.6.5). The third and

final steps are then dealt with separately for the supplemented behavioural profiles (section 3.6.6) and the simple behavioural profiles (section 3.6.7).

3.6.4 Legitimate interest

There is a commercial aspect to Bonnier News AB's interest in creating profiles to make the data available to affiliated companies in order for them to be used in tele marketing and postal direct marketing. IMY considers that the companies' interest is lawful, real and actually. In light thereof, IMY considers that the company's interest in creating profiles to make data available to affiliated companies in order to be used in tele marketing and postal direct marketing is legitimate.

3.6.5 Is the processing necessary for the legitimate interest?

The necessity requirement in Article 6(1)(f) of the GDPR must be examined in conjunction with the principle of data minimisation set out in Article 5.³² The purpose of the processing is to make contact information available to companies to use in tele marketing and postal direct marketing. The supervisory case has revealed that Bonnier News AB, together with the other companies, has taken steps to minimise the number of data collected and limit how long this data is processed, as well as to ensure that the databases in which the data are processed are kept separate and that only certain data are transferred in between. Furthermore, the company has ensured that no more information than what is necessary is disclosed to the affiliated companies in order to be used in tele marketing and postal direct marketing. In light thereof, IMY considers that the processing is necessary for the legitimate purpose.

3.6.6 Balance of interests for the processing of personal data in supplementary customer database profiles

Bonnier News AB has emphasised that the affiliated companies have an interest in marketing their products and services in an efficient and privacy-friendly manner. However, IMY points out that the interest in making data available for use in tele marketing and postal direct marketing is a commercial interest that does not weigh particularly heavily.

In the assessment of the interests of data subjects, IMY considers the following:

The profiling carried out on the supplemented customer database profiles includes data collected from affiliated companies during purchases and subscriptions (so-called customer engagements), data collection from Bisnode Sverige AB and data from the behavioural database (including data collected by the affiliated companies through cookies). IMY has already stated that Bonnier News AB should not have a greater possibility than the affiliated companies to rely on legitimate interest for the processing of personal data collected by the affiliated companies using cookies. The behavioural data of the data subject collected from the behavioural database to KDB is collected from the websites of different companies. IMY believes that data subjects cannot reasonably expect their behavioural data to be collected for marketing purposes just because they visit a website. Nor can reasonably expect their behavioural data to be combined with data from another purchase or collected data from other records for the purpose of being contacted for tele marketing or postal direct marketing. This does not change by the fact that the privacy-enhancing measure that the affiliates carrying out the marketing action do not have access to the collected behavioural data, but only contact details.

³² See judgment in Asociația de Proprietari bloc M5A-ScaraA, C-708/18, EU:C:2019:1064, paragraph 48

The EDPB guidelines show that the scope of legitimate interest as a lawful basis for profiling depends on the level of detail of the profile, the size of the profile, the impact of profiling and the safeguards designed to ensure a fair, non-discriminatory and accurate profiling process.

IMY considers that the privacy interest of data subjects is strong due to the nature of the data, as the data enables the identification of individuals' behaviour and the collection of the data is given special protection in LEK.

IMY further points out that this is profiling within the meaning of Article 4(4) of the GDPR and that profiling is extensive as it provides in-depth insight on the data subject. There is also the fact that these are data collected from different websites combined with data collected from customer engagements and statistical data from Bisnode Sverige AB. In light thereof, IMY notes that the nature of the processing means that the privacy interest of the data subjects weighs heavily.

In conclusion, IMY considers that the data subject's privacy interest outweighs Bonnier News AB's and affiliated companies' interest in the processing of personal data that is based on so-called supplemented customer database profile and that is done in order to make contact information available to affiliated companies for tele marketing and postal marketing.

In light thereof, IMY points out that Bonnier News AB has processed personal data without having a lawful basis for doing so pursuant to Article 6(1) GDPR by profiling the data subjects based on their supplemented customer database profiles in order to make contact information available to affiliated companies for tele marketing and postal marketing.

3.6.7 Balance of interests for personal data not linked to the behavioural database

As IMY stated above in section 3.6.6, Bonnier News AB's interest is primarily a commercial interest that does not weigh particularly heavily.

As regards the assessment of data subjects' interests in processing operations unrelated to the behavioural database, IMY takes into account the following: Bonnier News AB has taken steps to minimise the number of data points both in relation to the principles of data minimisation and storage minimisation by not sharing data at object level, but only by product category, brand and type of packaging. Profiling also does not include data collected through cookies. The investigation has also shown that the data subject has been given the opportunity to object before the processing is conducted and that Bonnier News AB respects the data subjects' wishes to avoid marketing that has been noted in national block lists or with the controller. In light thereof, IMY considers that the processing is within what private individuals can reasonably expect from the information provided and that the contact information is disclosed only to affiliated companies within the Group.

In conclusion, IMY considers that the interests or fundamental rights of the data subjects do not outweigh the interests of Bonnier News AB and the affiliated companies for the processing in question.

In light thereof, IMY notes that Bonnier News AB can rely on Article 6(1)(f) of the GDPR for the processing in question.

3.7 Choice of corrective measure

3.7.1 Applicable provisions etc.

In case of violations of the GDPR, IMY has a number of corrective powers, including reprimand, injunction and administrative fines. This follows from Article 58(2)(a) to (j) of the GDPR. IMY shall impose administrative fines in addition to or in place of other remedies referred to in Article 58(2), depending on the circumstances of each case.

If a controller or processor, with respect to one or the same or linked data processing operations, intentionally or negligently infringes several of the provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount determined for the most serious infringement. This is stated in Article 83(3) of the GDPR.

Each supervisory authority shall ensure that the imposition of administrative fines on a case-by-case basis is effective, proportionate and dissuasive. This is stated in Article 83(1) GDPR. Article 83(2) sets out the factors to be taken into account in order to determine whether an administrative pecuniary penalty is to be imposed and when assessing the amount of the fine.

The EDPB has adopted guidelines on the calculation of administrative fines under the GDPR aimed to create a harmonised methodology and principles for the calculation of fines.³³

In the case of a minor infringement, according to Recital 148 of the GDPR, instead of imposing a fine, IMY may issue a reprimand under Article 58(2)(b).

3.7.2 Same or interconnected data processing operations

In three cases above, IMY has assessed that Bonnier News AB had no lawful basis in Article 6(1) of the GDPR for its processing of personal data. IMY considers that these processing operations, all of which take place in the company's databases through profiling for marketing purposes, are linked within the meaning of Article 83(3) of the GDPR.

3.7.3 Administrative fine

IMY has assessed that Bonnier News AB has infringed Article 6(1) of the General Data Protection Regulation in its processing of personal data that takes place for the purpose of displaying personalised advertisements and to make contact information available to affiliated companies for tele marketing and postal direct marketing. IMY does not consider these to be minor infringements. Bonnier News AB shall therefore be subject to an administrative fine for these infringements.

IMY notes that breaches of Article 6(1) of the GDPR fall within the scope of Article 83(5), which means that an administrative fine of up to 20 million EUR or 4 % of the global annual turnover in the previous financial year, whichever is the highest, may be imposed.

In determining the maximum amount of an administrative fine to be imposed on a company, the definition of 'company' used by the Court of Justice of the European Union for the purposes of Articles 101 and 102 TFEU (see recital 150 of the GDPR). It

³³ EDPB Guidelines 8/2020 Guidelines 04/2022 on the calculation of administrative fines under the GDPR (adopted for public consultation on 12 May 2022).

is clear from the Court's case-law that this applies to any entity engaged in an economic activity, irrespective of its judicial form and the means in which it is financed, and even if, in the judicial sense, the entity consists of several natural or legal persons.³⁴

IMY assesses that the company's turnover to be used as a basis for calculating the administrative fine imposed on Bonnier News AB is Bonnier News AB's parent company Albert Bonnier AB. The information gathered shows that Albert Bonnier AB's annual turnover in 2021 was 23 299 000 000 SEK. The maximum amount that can be determined for the administrative fine in the case is four per cent of this amount, i.e. approximately 931 960 000 SEK.

IMY considers that the following factors are relevant for the assessment of the gravity of the infringement.

There has been a matter of profiling of private individuals for profit when the profiling has been carried out in order to display personalised advertisements as well as when it has been used to provide contact details for tele marketing and postal marketing.

The profiling that has been used to show personalised ads has, in cases where data in the behavioural database about private individuals' browsing behaviour have been linked to KDB, included browsing history, purchase history and demographic and statistical data. It has been a matter of an ongoing infringement involving a large number of data subjects and covering a large amount of personal data. However, the data processed do not constitute, as far as IMY has found, special categories of personal data as set out in Article 9 of the GDPR. In this decision, IMY considered that the profiling through supplementary behavioural profiles was extensive in nature.

Regarding the profiling of personal data in KDB where there was a link to data in the behavioural database, so-called 'supplemented customer database profiles', IMY has assessed that the profiling was extensive in nature, since it contained data collected about the private individual's browsing behaviour collected from several websites combined with data from purchases made (customer engagement) and data collected from Bisnode Sverige AB. However, IMY makes the assessment that the personal data processing at issue does not have major privacy implications for the data subjects. The impacts are considered moderate.

In both cases, IMY considers that the profiling carried out where data could be linked in the two databases, supplementary behavioural profiles and the supplementary customer database profiles, has a higher degree of gravity compared to the infringement related to the profiling carried out in the so-called 'simple behavioural profiles' for displaying personalised advertisements. IMY considers that the profiling that takes place in the so-called simple behavioural profiles for displaying personalised advertisements in itself constitutes grounds for an administrative fine, but that it has a lower degree of gravity than the infringements where a link between the different databases could be made. The reasoning behind this is that there is lesser data regarding the data subjects and that the natural person only can be identified indirectly. However, IMY takes into consideration that this infringement also includes systematic processing which has been ongoing for a long period of time and concerned a large number of data subjects.

³⁴ See judgment in Akzo Nobel, C-516/15, EU:C:2017:314, paragraph. 48

The measures taken by Bonnier to limit the infringement of the privacy of data subjects, in the form of retention periods, that data are not collected at product level, that no more data than necessary are disclosed to affiliated companies, have according to IMY, significantly reduced the gravity of the infringements. Also, the personal data has not been disclosed outside the Group. IMY has noted that Bonnier News AB has consistently taken steps to reduce the privacy infringement of the data subjects in its group common cooperation. This has also been taken into account when assessing the gravity of the infringements.

In the light of the above, IMY considers that all of these are infringements of lower seriousness. The starting point for the calculation of the administrative fine should therefore be low in relation to the current maximum amount.

In addition to the assessment of the gravity of the infringement, IMY must assess whether there are any aggravating or mitigating circumstances affecting the amount of the administrative fine. IMY considers that there are no additional aggravating or mitigating circumstances, other than those taken into account in the assessment of the seriousness above, which affect the amount of the fine.

In view of the gravity, aggravating and mitigating circumstances of the infringement and the high turnover in relation to the infringements found, IMY sets the administrative fine for Bonnier News AB at 13 000 000 SEK. IMY considers this amount to be effective, proportionate and dissuasive.

This decision has been taken by the Director-General [REDACTED] after a presentation by the lawyer [REDACTED]. In the final proceedings, the head of court [REDACTED] and the head of unit [REDACTED] also participated.

[REDACTED], 2023-06-26 (This is an electronic signature)

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's final decision 2023-08-09, no. IMY-2022-11493. Only the Swedish version of the decision is deemed authentic.

Ref no SE SA:
IMY-2022-11493

IMI case no:
164557

Ref no DE SA:
521.16340

Date of final decision:
2023-08-09

Final decision pursuant to Art. 60 under the General Data Protection Regulation – Klarna Bank AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Klarna Bank AB has now complied with the complainant's request for access. Furthermore, the complainant has stated that, in his view, the subject-matter of the complaint therefore is closed. Against this background, IMY finds no reason to take further action in the case.

The case is closed.

Presentation of the case

The complainant lodged a complaint with the German Data Protection Authority (Berlin Commissioner for Data Protection and Freedom of Information) against Klarna Bank AB (Klarna) alleging, inter alia, that Klarna had failed to handle the complainant's request for access under Article 15 of the General Data Protection Regulation.

The complaint has been submitted to IMY, as the lead supervisory authority under Article 56 GDPR, in accordance with the Regulation's provisions on cooperation in cross-border processing.

The complainant subsequently stated by email to the German Data Protection Authority on 14 December 2022 that Klarna has now fully complied with the complainant's request for access. The complainant further explained that, in his view, the subject-matter of the complaint is therefore closed.

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

Statement of reasons for the decision

It is apparent from the information in the case that Klarna has taken steps to satisfy the complainant's right of access and that the complainant himself considers that the subject-matter of the complaint therefore is closed. Against this background, IMY does not find any reason to take further action in the case.

The case should therefore be closed.

Notice: this document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) final decision in case with national reference number, DI-2021-9842. Only the Swedish version of the decision is deemed authentic.

Registration number:
DI-2021-9842

Date:
2023-08-03

Decision under the General Data Protection Regulation- Jollyroom AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Jollyroom AB (556815-7159) has processed the complainant's personal data in breach of Article 32(1) of the General Data Protection Regulation (GDPR)¹ by failing to take appropriate technical and organisational measures to ensure adequate protection against unauthorised disclosure on its website for personal data in the complainant's customer profile.

The Authority for Privacy Protection issue Jollyroom AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 32(1) of the GDPR.

Report of the supervisory report

Handling

The Swedish Authority for Privacy Protection (IMY) has initiated supervision regarding Jollyroom AB due to a complaint. The complaint has been submitted to IMY, as lead supervisory authority under Article 56 GDPR. The handover has been made by the supervisory authority of the country where the complainant has lodged his complaint (Denmark) in accordance with the Regulation's provision on cooperation in cross-border processing.

The investigation at IMY has been carried out thorough correspondence. In the light of a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency provided for in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Finland, Norway and Germany.

The complaint

It is stated in the complaint that on 6th of November 2019 there was a security flaw on Jollyroom AB's Danish website. The complainant has observed that it was possible for him to log in to Jollyroom's customer service function using only email and zip code.

Mailing address:
Box 8114

104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

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).

There was therefore no need for a password or other identification method for logging in. After the complainant has logged in with the new method, he could see the individual's profile including; name, e-mail, telephone number and address.

What Jollyroom AB has stated

Jollyroom AB has mainly stated the following.

The company is the controller for the processing to which the complaint relates.

The complainants description is true in all relevant aspects. The incident has been a consequence of a bug in the system and has not been a deliberate implemented functionality on the website. Due to unforeseen technical problems, the functionality ended up outside the general customer profile logic with login requirements. The functionality was intended for those who were logged in to their customer profiles. This functionality was implemented unintentionally and has not allowed access to the entire customer profile, but only to the following categories of data. Name, email address, telephone number, address, postcode and postal location. This security flaw has not given access to all the categories of data available in regular logged-in mode, thus no order history has been exposed.

The company's website incorporates other commonly used security mechanisms such as password requirements for access to customer data and encrypted transport protocols for data traffic.

The current system has been replaced.

Justification of the decision

Applicable provisions

Article 32 regulates the security of the processing. Paragraph 1 requires the controller, taking into account the latest developments, the costs of implementation and the nature, scope, context and purpose of the processing as well as the risks, of varying probability and severity, to the rights and freedoms of natural persons, to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

According to Article 32(2), when assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the personal data transmitted, stored or otherwise processed.

Assessment of the Authority for Privacy Protection (IMY)

IMY notes, first of all, that Jollyroom AB, has taken steps to ensure that the individual's data are now password protected.

However, IMY has found that the exposure of the complainant's personal data was possible through its non-intentional functionality, the complainant's personal data did not have sufficient protection against unauthorised disclosure. In IMY's assessment, the lack of adequate protection should have been discovered before the controller started processing personal data. IMY considers that Jollyroom AB has not taken

appropriate technical and organisational measures pursuant to Article 32(1) to ensure adequate protection against unauthorised disclosure on its website for personal data in the complainant's customer profile. Jollyroom AB has thus processed personal data in breach of Article 32(1) of the General Data Protection Regulation.

Choice of intervention

It follows from Article 58(2) of and Article 83(2) of the GDPR that IMY has the power to impose administrative fines in accordance with Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine issue a reprimand pursuant to Article 58(2) (b). Factors to consider is the aggravating and mitigating circumstances in the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The supervision covers the processing of an individual complainant's personal data in the situation to which the complaint relates. The infringement was committed negligently. Neither sensitive nor integrity-sensitive data have been involved. Furthermore, the company has taken measures to protect information against unauthorised disclosure. IMY has not previously established that the company has infringed the GDPR.

Against this background, IMY considers that it is a minor infringement within the meaning of recital 148 and that Jollyroom AB should be reprimanded pursuant to Article 58(2)(b) GDPR.

This decision has been taken by Acting Head of Unit for [REDACTED] after a presentation by the legal expert [REDACTED].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority's contact information is shown in the first page of the decision.



REPUBLIC OF SLOVENIA

INFORMATION
COMMISSIONER

Dunajska cesta 22, 1000 Ljubljana

T: 01 230 9730

www.ip-rs.si

gp.ip@ip-rs.si

National number: 0611-394/2021

IMI Case Register entry: 512935

Date: 9. 2. 2024

The Information Commissioner (hereinafter referred to as: IP) hereby issues, under the State Supervisor for Personal Data Protection [REDACTED], on the basis of Articles 2 and 8 of the Information Commissioner Act (Official Journal of the Republic of Slovenia, No. 113/2005, with amendments and additions; hereinafter referred to as: ZInFP), Articles 36, 37 and 119(1) of the Personal Data Protection Act (Official Journal of the Republic of Slovenia, No. 163/22; hereinafter referred to as: ZVOP-2), Article 135(4) of the General Administrative Procedure Act (Official Journal of the Republic of Slovenia, No. 24/06 — UPB2, 126/07, 65/08, 8/10, 82/13, 175/20 — ZIUOPDVE and 3/22 — Zdeb; hereinafter referred to as: ZUP) in conjunction with Article 3(2) of the Inspection Act (Official Journal of the Republic of Slovenia, No. 43/07 — UPB1 and 40/14; hereinafter referred to as: ZIN) and Article 56(1) of 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; hereinafter referred to as: GDPR), in the matter of carrying out inspection of the implementation of the provisions of the GDPR and the ZVOP-2 at [REDACTED] (hereinafter: the controller), ex officio the following

DRAFT DECISION

1. The inspection procedure conducted by the IP at the controller [REDACTED] [REDACTED], under national No. [REDACTED], in which the controller voluntarily rectified all illegalities, irregularities and deficiencies found during the procedure, is closed.
2. No specific costs have been incurred by the authority and the controller bears his own costs of the proceedings.

Findings and reasoning

The inspection procedure was conducted by the IP, on the basis of the received complaint, filed by the Hungarian individual ([REDACTED]) at the Hungarian Competition Authority and then transferred to the Hungarian Data Protection Authority (hereinafter referred to as: Hungarian DPA). The complaint in question gave rise to allegedly inadequate security of the payment card data and a request for deletion of the data of the complainant, which were indicated by the complainant when entering the data on the purchase of the item on the website [REDACTED].

On 6 July 2021, the Hungarian DPA launched, via the Internal Market Information System (hereinafter: IMI), under the cooperation mechanism provided for in the GDPR, the procedure for the identification of a lead supervisory authority in accordance with Article 56 of the GDPR. It was established that the sole place of establishment of the controller is in [REDACTED] and that the processing significantly affects or could significantly affect individuals in more than one Member State, since the controller, in addition to the online store at [REDACTED], also manages online shops at [REDACTED], [REDACTED], [REDACTED] and [REDACTED]. Therefore, IP confirmed, through IMI system, on 19 July 2021, that it will conduct the procedure as the lead supervisory authority (hereinafter referred to as: LSA).

Within the framework of the cooperation mechanism, the IP forwarded preliminary draft decision on the 5 June 2023 to the concerned supervisory authorities for an opinion (according to procedure A61VMN 513203), in connection with which the Hungarian supervisory authority forwarded comments. Taking into account the comments of the Hungarian supervisory authority, the IP issued a draft decision on 29 December 2023 (according to procedure A60 DD 591435) and forwarded it to the relevant authorities for their opinion, but did not receive any comments to it.

The investigation conducted by the IP concerned two issues, namely (1) whether the controller complied with the request of the complainant for deletion of his personal data; and (2) whether controller ensured appropriate level of security of personal data processed in relation to payment cards.

According to the information indicated in the complaint, the IP firstly investigated the controller's website (doc. No 0611-394/2021/4 of 13.10.2021) and asked him to provide written explanations, documentation and statements (doc. 0611-394/2021/5 of 30.11.2021). In its request, the IP briefly explained to the controller the procedure for cooperation between supervisory authorities in accordance with the procedure laid down in Article 60 of the GDPR.

Regarding the complainant's data in the present case, the controller on 21 December 2021 (doc. No 0611-394/2021/6) explained that personal data relating to him are no longer stored. If it were stored and the data was entered from an unfinished purchase process, it would not be a systemic error, but rather a result of functionality embedded in the website (so-called "abandoned cart" functionality).

On 22 November 2022 the IP requested the controller to provide additional explanations, documentation and statements (doc. No 0611-394/2021/7), to which the controller replied on 7 December 2022 (doc. No 0611-394/2021/8). In its reply, the controller provided a more general description of the procedure for the erasure of personal data at the request of an individual.

Additionally, on 13 April 2023 the IP requested the controller (via its DPO) to provide a contract between the controller and the company [REDACTED], which provides online payment card processing for the controller (doc. No 0611-394/2021/9). The controller sent the requested contract to the IP the same day (doc. No 0611-394/2021/10).

Based on the explanations and documentation provided by the controller, the IP summarises the key findings of the investigation procedure:

I. Regarding a request for the erasure of all personal data processed by the controller in relation to the complainant

Article 17 of the 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 for the purposes for which they were collected or otherwise processed;*
- (b) the data subject withdraws consent on the basis of which the processing takes place pursuant to point (a) of Article 6 (1) or point (a) of Article 9 (2), and where there is no other legal basis 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 must be erased in order to comply with a legal obligation pursuant to Union or Member State law to which the controller is subject;*

(f) the personal data have been collected in connection with the provision of information society services referred to in Article 8 (1).

It is apparent from the documentation obtained that the complainant [REDACTED] received on 11 October 2020 a message from the e-mail address [REDACTED] about the placed order ([REDACTED]) with a summary of the order placed on the type of goods ordered, discount, final price, VAT, handling costs, delivery address, billing address, delivery method and method of payment.

The complainant [REDACTED] replied on the same day (11 October 2020) to the e-mail address [REDACTED], that he did not place the order [REDACTED], but only browsed the controller's website and therefore requested the deletion of the order and all personal data relating to him as well.

The controller also replied on the same day (11 October 2020), from the e-mail address [REDACTED], that there was most likely a systemic error and that his order had been cancelled and the data deleted.

On 13 October 2020 the complainant received an advertisement from [REDACTED] and then again on 15 October 2020. Therefore, the complainant sent another request for the deletion of all his data from the controller's system (on 15 October 2020), to the e-mail address [REDACTED] and received a reply that his e-mail address had been deleted from the messaging (marketing) system. After that date, the complainant did not receive any advertising messages from the controller anymore.

In its reply of 11 February 2021 to the Hungarian DPA, the controller confirmed, that the complainant [REDACTED] had indeed requested the deletion of the order and any personal data relating to him on 11 October 2020, by e-mail [REDACTED]. The controller immediately complied with his request and replied on the same day that he had deleted his data. He admitted that the complainant had indeed received an e-mail of a commercial nature. Consequently, on 15 October 2020 the controller deleted his e-mail address also from the list of e-mail addresses and informed the individual thereof on the same day. He added that there was probably a systemic error in the conclusion of the order, since the system recorded the order as concluded, even though the individual [REDACTED] did not click on the 'Submit order' button. However, the controller also allowed the possibility for the complainant to actually conclude the order by himself. On the fact that no data relating to the order placed by a complainant or data relating to him, are no longer present in the controller's system, the controller submitted screenshots of its databases.

On 21 December 2021, the controller, upon the request of the IP (doc. No 0611-394/2021/5 of 30.11.2021), again confirmed, that he does not retain any data concerning the complainant [REDACTED], with e-mail address [REDACTED].

Upon the request of the IP (doc. No 0611-394/2021/7) the controller on 7 December 2022 provided a more general description of the procedure for the erasure of personal data at the request of an individual. The controller explained that individuals rarely submit such a request, however, where appropriate, the controller complies with it. The controller further explained, that its contractor [REDACTED], which provides hosting and operation of the online store and operation of the cash register, provides the functionality of deleting all data about a particular user by clicking ("Erase personal data"), about which the controller has also attached a screen image. The controller then informs the other processors of the deletion by e-mail.

II. Concerning the suspicion of inadequate protection of personal data relating to the processing of personal data by payment cards

The complainant stated that personal data related to the payment card are processed directly on the website [REDACTED] and not via the secure platform to which the individuals are supposed to be redirected at the stage of entering payment card data. With regard to his allegation, the complainant did not provide any evidence.

The controller explained that the data related to the online payments are not processed on the website [REDACTED], but is carried out through the [REDACTED] system which ensures adequate security of personal data. Attached agreement ("[REDACTED]") indicated that the agreement was concluded on [REDACTED] with [REDACTED].

On 17 December 2021, upon the request of the IP, the controller added, that in relation to the payments processing it has a signed agreement with its external partners [REDACTED] and [REDACTED] [REDACTED] in order to ensure the processing of online payments by payment cards. The Agreement ([REDACTED]) has been attached by the controller to its explanations. However, as the agreement was allegedly extracted from the [REDACTED] system, there was no indication of the date that the agreement had been concluded on. Therefore, the IP requested additional evidence that would support the allegation of the controller with regard to the online payments system.

On December 8 2023 the controller provided additional explanations regarding the validity of the [REDACTED] Service Agreement. In this regard the controller explained that the [REDACTED] service has been used since 20 January 2021 (in this regard the controller enclosed the printout of all payments from the [REDACTED] system). However, the contract with [REDACTED] and [REDACTED] had been terminated lately on 14 October 2021 and as evidence the controller attached a document "Notice to terminate the [REDACTED] Agreement".

According to the findings, in relation to the secure payments processing, at the time of the alleged purchase by [REDACTED] on 11 October 2020, the controller used the services of [REDACTED], and [REDACTED], and no evidence was found in the inspection procedure that would make it possible to impose responsibility to the controller of inadequate security of personal data related to the payment cards and, therefore, of an infringement of Article 32 of the GDPR.

To conclude, in a view of the above-mentioned measures of the controller, by which it has rectified the non-compliances revealed ex officio within the investigation procedure and specifically, non-compliance with Article 17 of the GDPR, deleting the requested data of the complainant [REDACTED], thereby established a legitimate processing of personal data, IP concludes that, in the present case, it would be appropriate to continue the inspection procedure only if the inspection measure was necessary to order the correction of deficiencies and irregularities in relation to the processing of personal data or to order the prohibition of unlawful processing of personal data and to establish a legitimate processing for the future. In the specific case, all irregularities found in the course of the investigation procedure were rectified, therefore, in accordance with the fourth paragraph of Article 135 of the ZUP, in conjunction with the second paragraph of Article 3 of the ZIN and Article 2 of the ZInfp and Articles 57 and 58 of the GDPR should be closed, as is apparent from point 1 of the operative part of this Decision.

Under the third paragraph of Article 118 of the ZUP, the costs of the proceedings are to be decided in the decision terminating the proceedings. In the present proceedings, no special costs have been incurred, as is apparent from point 2 of the operative part of this Decision.

This Decision is issued ex officio and on the basis of Article 22 of the Administrative Fees Act (Official Journal of the Republic of Slovenia No. 106/10 — official consolidated text, 14/15 — ZUUJFO, 84/15 — ZZelP-J and 32/16) the fees are free.

Instruction on Remedies: There is no appeal against this decision, but an administrative dispute is allowed. The administrative dispute is initiated by an action, which is filed within 30 days of service of the decision at the Administrative Court of the Republic of Slovenia, Fajfarjeva 33, 1000 Ljubljana. The application is sent by registered mail to that court. The action, accompanied by any annexes, shall be filed at least in triplicate. The application must also be accompanied by this order in original or transcript.

[REDACTED]
State Supervisor for Personal Data Protection

Recipient:

- [REDACTED]



REPUBLIKA SLOVENIJA

INFORMACIJSKI
POOBLAŠČENEC

Dunajska cesta 22, 1000 Ljubljana

T: 01 230 9730

www.ip-rs.si

gp.ip@ip-rs.si

IMI Case Register entry: 492052 (in connection with A56 454116)

Ref. Nos. in National Systems: NAIH-7117/2022, 07141-6/2023/14

Date: 5 December, 2024

The Information Commissioner (hereinafter: the IP) issues, under the Personal Data Protection Supervisor, on the basis of Article 77 of 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 (the General Data Protection Regulation; hereinafter: the GDPR) and Article 34 in relation to point 2 of paragraph 1 of Article 55 of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 163/22; hereinafter: ZVOP-2) and conjunction with the General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, No. 24/06 – official consolidated text, as amended; hereinafter: ZUP) in the complaint procedure of the complainant: [REDACTED]

[REDACTED] Hungary, dated 26 August 2022, against the controller: [REDACTED]
[REDACTED], in the matter of the right to erasure of personal data

FINAL DECISION¹

1. It is established that the controller [REDACTED], d.o.o. infringed Article 17 in conjunction with Article 12 of the GDPR at the time of filing of the complaint by the complainant [REDACTED] [REDACTED] on 26 August 2022, by failing to take a timely and appropriate decision on the request for erasure of personal data.
2. No measures are ordered against the controller [REDACTED] regarding the processing of personal data of the complainant [REDACTED].
3. The complainant [REDACTED] is granted full access to the case file No. 07141-6/2023.
4. In this procedure, the authority did not incur any special costs, and each party covers its own costs of the procedure.

Statement of grounds:

The proceedings to date and relevant submissions made by the parties

The IP received a request from the Hungarian supervisory authority Nemzeti Adatvédelmi és Információszabadság Hatóság (hereinafter: the Hungarian supervisory authority) in the context of the procedure for determining the lead supervisory authority under Article 56 of the GDPR to supervise the legality of the processing of personal data i.e. the complaint, filed by complainant [REDACTED] [REDACTED]. The complaint states that the complainant registered an account in her own name on the web portal [REDACTED] providing in addition her email address and phone number at the time of registration. On the same day, she wanted to terminate or delete her account, which the website itself

¹ Unofficial translation for the purpose of issuing Final Decision in A6O procedure.

did not enable. She therefore sent a request for the deletion of her personal data to the controller indicated in the privacy policy of the website in question, to [REDACTED] at the e-mail address [REDACTED] on 31. 5. 2022. In the complaint filed with the Hungarian supervisory authority on 26 August 2022, the complainant further states that she has not received any response from the controller.

After reviewing the complaint, the IP has, in accordance with Articles 9 and 141 of General Administrative Procedure Act (Official Gazette of the Republic of Slovenia, No. 24/06 – official consolidated text, as amended; hereinafter: ZUP) in relation to Article 25 of Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 163/22; hereinafter: ZVOP-2) and in accordance with the powers from Article 28 of ZVOP-2 and Article 58 of the GDPR, asked the controller on 20 March 2023 to either provide a response on the statements of the complainant or to issue a written decision on the complainant's request in accordance with Articles 12 and 17 of the GDPR in relation to Article 14 of ZVOP-2.

The controller replied within the set deadline on 5 April 2023 stating that on 31 March 2023 it deleted the complainant's account and all personal data relating to it and informed the complainant thereof. The letter to the complainant has been attached to the reply. In the reply, the controller further explained that the irregularity occurred due to an unintentional human error, as the employee, to whom the email with the deletion request was addressed, had just left her job during the period in question.

On 13 April 2023, the IP sent a notification to the Hungarian supervisory authority informing the complainant of the response of the controller and inviting her to clarify whether she had received the deletion notice and whether she maintains the complaint.

On 12 May 2023, the complainant replied that she maintains the complaint and wanted an official decision from the supervisory authority on the controller's violation of the GDPR.

On this basis, the IP issued a record of findings essential for the decision in this procedure together with a call for a statement before the decision, which it forwarded to the controller on 6 February 2024, and was forwarded to the complainant by the Hungarian supervisory authority on 21 February 2024. In the record, the IP found that the controller had violated Article 17 in conjunction with Article 12 of the GDPR at the time of filing the complaint. However, since the controller had remedied the infringement after the request by performing the erasure and notifying the complainant, the IP shall not impose any special measures related to the processing of personal data of the complainant. No party responded to the call within the set 10-day period from the date of service.

Since the IP considered that the facts of the case had been fully established, it did not carry out any other procedural steps.

Supervisory procedure

Paragraph 1 of Article 30 of the ZVOP-2 provides that an individual who believes that the processing of his/her personal data by a controller or a processor infringes the provisions of the GDPR, this Act or other laws governing the processing or protection of personal data, or infringes the provisions of related implementing regulations or general acts, may submit a request to the supervisory authority in accordance with the law governing the general administrative procedure, requesting supervision of the lawfulness of the processing of his/her personal data, and may also propose the necessary action to

be taken in accordance with the previous Article in case of established violations, so as to achieve the restoration of the lawful situation. The second paragraph of the same Article of ZVOP-2 stipulates that each party bears its own costs of the proceedings.

Therefore, the IP dealt with the application in a procedure conducted at the request of the complainant with a special status, which guarantees the right to appeal under Article 77 of GDPR. In this supervisory procedure, it acted according to the provisions of Articles 30 to 35 of ZVOP-2 (procedure based on the application of a complainant with a special status). Among other things, this procedure is characterized by the fact that the IP acts in accordance with the investigative and regulatory powers established in Article 58 of the GDPR and Articles 28 and 29 of ZVOP-2 and in accordance with the general rules of administrative procedure act.

After the supervision procedure, the IP, as a supervisory authority, issues a decision in accordance with paragraph 1 of Article 34 of the ZVOP-2. Such a decision, in addition to the elements specified by the law governing the general administrative procedure, contains:

- 1) determination of the existence or non-existence of the alleged infringement of the processing of personal data of the complainant with a special status at the time of filing the complaint;
- 2) measures ordered against the controller or processor regarding the processing of personal data relating to the complainant with a special status, and the deadline for their implementation;
- 3) permitted scope of review of the case file for a complainant with a special status.

On the right to erasure of personal data

Pursuant to Article 17(1) of the GDPR, the data subject shall have the right, in the exhaustively listed cases, to obtain from the controller the erasure of personal data relating to her/him without undue delay, and the controller shall have the obligation to erase the personal data without undue delay.

The controller shall provide the data subject the information on action taken on a request under Articles 15 to 22 of the GDPR without undue delay and in any event within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay (Article 12(3) of the GDPR). If the controller does not take action on the data subject's request, it shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (Article 12(4) of the GDPR).

Assessment of statements made by the complainant

The IP finds that at the time of filing of the complaint with the Hungarian supervisory authority, i.e. on 26 August 2022, the controller has not yet decided on the complainant's request of 31 May 2022 to delete her personal data. This is confirmed also by the statement of the controller. As the one-month deadline for a decision on the erasure request expired, the IP considers that the controller infringed Article 17 in conjunction with Article 12 of the GDPR at the time of filing of the complaint and decides as set out in point 1 of the operative part of this decision. However, this infringement was immediately remedied by the controller after the filing of the complaint and the request by the IP, by deciding on the complainant's request, granting it and deleting her data, as evidenced by the controller's notice of deletion sent to the complainant and its response sent to the IP on 5 April 2023.

The IP set out these findings, which are essential for the decision in the present proceedings, in the record and asked the parties to comment on the findings, in accordance with Article 32(2) and Article 33(2) of ZVOP-2. No party responded to the call. The IP considered that the controller completely remedied the identified infringement of the right to erasure of personal data by granting the complainant's request, deleting the requested personal data and informing the complainant thereof in writing. Therefore, the IP did not order the controller to take particular measures in relation to the processing of the complainant's personal data (point 2 of the operative part of the decision), since the irregularities found in the processing of the complainant's personal data no longer exist at the time of the adoption of this decision.

Permissible scope of revision of the case file

Point 3 of paragraph 1 of Article 34 of ZVOP-2 stipulates that the decision in the procedure according to the provisions of this section, in addition to the elements specified by the law governing the general administrative procedure, also contains the permissible scope of revision of the case file for the complainant with special status.

The IP did not restrict the complainant's right to review the file of the case, which is kept under no. 07141-6/2023, as there are no reasons justifying such a restriction (point 3 of the operative part of the decision).

Costs

Pursuant to the paragraph 1 of Article 118 of ZUP, the authority shall decide on the costs of procedure, on who is to bear the costs of procedure, on the amount thereof and on whom and in what time limit they are to be paid by a decision.. No special costs were incurred in this procedure. Pursuant to the paragraph 2 of Article 30 of ZVOP-2, the complainant and the controller shall each bear their own costs that they may incur as a result of the procedure, which led the IP to take the decision as set out in point 4 of the operative part of this decision.

In accordance with the provisions of the Administrative Fees Act (Official Gazette of the Republic of Slovenia, No. 106/10 - official consolidated text, as amended), this decision is exempt from the payment of administrative fees.

Instruction on legal remedies:

An appeal against this decision is not permissible, but an administrative dispute may be initiated against the decision. An administrative dispute may be brought by filing an action with the Administrative Court of the Republic of Slovenia, Fajfarjeva 33, 1000 Ljubljana. The action must be filed within thirty days from the service of this decision, either in writing directly to the said court or by registered mail or orally on record. In addition to the original, transcript or copy of this decision, the action must also be accompanied by one transcript or copy of the action and attachments for the defendant, if someone is affected by the decision, than one as well for him or her.

[REDACTED]
State Supervisor for Personal Data Protection

Recipients:

1. Complainant: [REDACTED] – served by the Hungarian supervisory authority,
2. Controller: [REDACTED]

[REDACTED].



National No. 00211/2022-Os-3 (prev. 00499/2021-Os-7)
IMI Art.56: 178247
Case register no. 187706

In Bratislava, Slovakia

06.06.2022

Official record

to postpone the complaint pursuant to Sec. 100 (5) of the Act no. 18/2018 Coll. on Personal Data Protection and amending and supplementing certain Acts (hereinafter as „Slovak Data Protection Act“)

On February 2, 2021 the Lithuanian Supervisory Authority (State Data Protection Inspectorate) (hereinafter as “Lithuanian SA”) contacted the Office for Personal Data Protection of the Slovak Republic (hereinafter as “Slovak SA”) via the internal IMI system (Art. 56, no. 178247 - identification of LSA and CSA procedure).

Lithuanian SA received a complaint from (hereinafter as „complainant“) against the controller established in Slovakia: **JOO INTERNET MEDIA LTD, organizačná zložka, Tallerova 4, 811 02 Bratislava, company registered no. 47 079 932** (hereinafter as „controller“). The complainant claims that the controller makes complainant’s personal identification number publicly available on its website www.joolist.eu.

After the examining the case, the Slovak SA decided on the basis of the provisions of Sec. 100 (5) (a) of Slovak Data Protection Act to **postpone** the complaint (no. 00211/2022-Os, prev.00499/2021-Os, IMI no A56 178247, Case register 102666).

REASONING

On February 2, 2021, the Lithuanian Supervisory Authority contacted Slovak SA via the internal IMI system (Art. 56, no. 178247 - identification of LSA and CSA procedure).

Lithuanian SA received a complaint from the complainant against the controller established in Slovakia. The complainant claims that the controller makes complainant’s personal identification number publicly available on its website www.joolist.eu.

The complainant in his complaint states that when the name and surname, i.e. , is entered in Google search engine, the personal identification number of the complainant is publicly available on controller’s website.

The Lituanian Supervisory Authority asked the Slovak SA due to March 4, 2021 to state whether the Slovak SA would act as LSA in this matter in question. After a preliminary vetting of the complaint, the Slovak SA stated that the controller states on the website www.joolist.eu that it has its main establishment in the United Kingdom (Suite 126 Higham Hill JSC, 313 Billet road, E17 5PX London), but its main place of business is in the Slovak Republic. Based on the information available Slovak SA has assumed its role as LSA.

In the complaint, the complainant stated that he had evidence of the disclosure of his data, but this evidence was not submitted through IMI. Slovak SA was also unable to determine



the scope of the objected data, as the complainant objected disclosure of the “Personal identification number”.

Therefore, before the confirmation of the Slovak SA's role as LSA, the Slovak SA requested the Lithuanian SA to provide the evidence mentioned by the complainant in his complaint and to specify what the complainant means by “personal identification number”. On March 8, 2021, the Lithuanian Supervisory Authority attached the required information with a link to the website <https://www.joolist.eu/> as well as the screenshot of the Google search engine. After examining the evidence, the Slovak SA confirmed to act as LSA and created Case register no. 187706.

The Slovak SA requested the controller for cooperation, in particular to indicate whether it processes the complainant's personal data and if so, to what extent, for what purpose and on what legal basis data is processed; to indicate whether the controller has published the identity of the complainant on the website www.joolist.eu and if so, what is the legal basis and purpose of such publication. Slovak SA also asked the controller whether the controller was contacted by the complainant with a request to erasure his personal identification number and if so, to provide the evidence and, if the controller has dealt with the request to provide the evidence for doing so as well.

The controller answered, quote (unofficial translation): "*Our company does not process the complainant's personal data in the databases but registers this data as the name of the company. We register 1 job offer, which is publicly available in five languages. We obtained this job offer from freely available gateways provided by the regional employment offices in each country in the European Union, which are part of and provide this data to the European Job Mobility Portal EURES. Our company does not process personal data (in English "personal identification number") of the complainant in its databases, but we register the name of the company in the section Employer as a job offer looking for hostesses, mannequins. We were not contacted by complainant via the email address info@joolist.eu or gdpr@jooteam.eu (<https://www.joolist.eu/sk-sk/osobne-udaje-gdpr/privacypolicy>). Complainant with request to erasure the complainant' data did not contact us in our profile via the Facebook, to which our website is linked with. Complainant with request to erasure the complainant' data did not contact us via our web form on www.jooteam.eu, which is linked to the website www.joolist.eu. We were not contacted by Google Search Console to delete the links in the search engine. We deleted this job offer and requested the Google Search Console to erasure the searching index.*"

Pursuant to Recital 14 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 (General Data Protection Regulation) (hereinafter as „GDPR“), the protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. This Regulation does not cover the processing of personal data, which concerns legal persons, and in particular, undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person.



Pursuant to Art 4 (7) GDPR, for the purposes of this Regulation: ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Pursuant to Art. 4 (23) GDPR, for the purposes of this Regulation: ‘cross-border processing’ means either:

- (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Pursuant to Art. 15 GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Pursuant to Art. 17 GDPR, 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).

Pursuant to Art 56 (1) GDPR, without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

Pursuant to Art 56 (2) GDPR, by derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

The purpose of personal data protection proceeding in Slovak Republic (hereafter as “proceeding”) is to determine whether there was any infringement of the rights of natural persons when their personal data were processed or if there was any violation to this Act or GDPR in the area of personal data protection; and, if any deficiencies are identified, if it is reasonable and useful, to impose corrective measures or impose a fine for violation of this Act or GDPR .

Pursuant to Sec. 100 (1) of the Slovak Data Protection Act, the proceeding is initiated based on the complaint of a data subject that claims that his or her rights lay down by this Act are directly influenced (hereafter as “the complainant”), or without a complaint.

Pursuant to Sec. 100 (5) (a)of the Slovak Data Protection Act, (5) The Office shall postpone the complaint if the complaint is manifestly unfounded.

The controller declared to the Slovak SA that the controller does not process any data of the complainant in its databases, but the controller registered the complainant as the legal person in the Employer's section. The controller further stated that complainant did not contact him to erasure the complainant's data. The controller deleted the publicly available job offer together with the data that had been published on www.joolist.eu. The controller also requested the Google Search Console to erasure the searching index for the name

The Slovak SA verified the abovementioned statements of the controller on September 24, 2021. The findings of the Slovak SA are: on the website <https://www.joolist.eu/>, there is no data of the complainant publicly available, the name and surname of the complainant in connection with the website www.joolist.eu is not publicly available in Google search engine either.



On the basis of abovementioned findings, the Slovak SA decided to postponed the complaint pursuant to Sec. 100 (5) (a) of the Slovak Data Protection Act without launching an administrative proceeding.

Should new relevant facts be identified, the matter could be reviewed in the personal data protection proceedings.

Head of the Department
of administrative proceedings
Office for Personal Data Protection
of the Slovak Republic



No. 01403/2021-Os-1 (previously 00418/2020-Os)
IMI Art.56: 87443
Case register no. 102666

In Bratislava, Slovakia
15.07.2022

Official record

to dismiss the complaint pursuant to Sec. 100 (5) of the Act no. 18/2018 Coll. on Personal Data Protection and amending and supplementing certain Acts in wording of the Act no. 221/2019 Coll. (hereinafter referred as „Slovak Data Protection Act“)

On November 5, 2019 the Slovenian Supervisory Authority (Information Commissioner of the Republic of Slovenia) (hereinafter referred to as “Slovenian SA”) contacted the Office for Personal Data Protection of the Slovak Republic (hereinafter the “Slovak SA”) via the internal IMI system (Art. 56, IMI no. 87443 - identification of LSA and CSA procedure).

Slovenian SA received a complaint from a Slovenian citizen – [REDACTED] (hereinafter referred as „[REDACTED]“ or „data subject“) against FC ecom, s.r.o. **Veľkomoravská 2866/9, 911 05 Trenčín, Slovakia, company registered no. 51 750 155** (hereinafter referred as „controller“ or „FC ecom, s.r.o.“), controller established in Slovakia. The complainant claims that he exercised his right of access [Article 15 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 (General Data Protection Regulation) (hereinafter as „GDPR“)], but the controller refused to act on the request of the data subject within one month.

After examining the case, the Office has come to the conclusion that the complaint is manifestly unfounded, and therefore on the basis of the provisions of Sec. 100 (5) (a) of Slovak Data Protection Act, the Slovak SA has decided to **dismiss** the complaint [no. 01403/2021-Os-1 (previously 00418/2020-Os), IMI no. A56 87443, Case register 102666].

REASONING

On November 5, 2019 the Slovenian Supervisory Authority contacted the Slovak SA via the internal IMI system (Art. 56, no. 87443 - identification of LSA and CSA procedure). Slovenian SA received a complaint from a Slovenian citizen against FC ecom, s.r.o., controller established in Slovakia. The controller runs an online store that is also available in Slovenian language for Slovenian customers (<https://si.factcool.com>). The complainant claims that he exercised his right of access (article 15 of the GDPR), but the controller refused to act on the request within one month. The controller replied to the request but it did not provide the complainant with any relevant information regarding the processing of his personal data nor did the controller refuse the request.

The complainant in his complaint stated, quote: „*On 19.08.2019 I sent an e-mail to FACTCOOL S.R.O. to factcool-si@factcool.com requesting access to my personal data in accordance with Article 15 of the GDPR. I received the letter below dated 22.08.2019 which*



I am forwarding to you. Their reply and the information provided is not in line with the GDPR, I insist that the company should inform me where it obtained my personal data. It is obvious that my personal data was exported to other countries without my knowledge. This is misuse of my personal data. The reply of the company has nothing to do with my request to Access personal data. I am asking the Information Commissioner of the Republic of Slovenia to consider my complaint as a priority. A also notified Agency for Communication Network and Services of the Republic of Slovenia and in the next few days I am planning to file a lawsuit with the Administrative Court of the Republic of Slovenia against the company. Because of that I ask you to consider the matter as a priority. If needed you should communicate with the Data Protection Authority of Slovakia as the company has its headquarters there.“

The complainant exercised his right to access to his personal data on August 19, 2019 via e-mail address to the controller. The controller sent its reply on August 22, 2019 with the following, quote: „Factcool s.r.o. (Slovakia) sold Factcool.com online store to FC Ecom s.r.o. (Slovakia). Until 01.10.2018, Factcool s.r.o. only sold goods in Slovakia. In Slovenia, Factcool ltd from United Kingdom sold the Factcool.com online store. FC Ecom s.r.o. does not have any customer data from Factcool ltd. Factcool ltd owns the data. Attached to this email you will find a document about the sale of the company.“

According to the findings of the Slovak SA, FC ecom s.r.o. operates an online store <https://sk.factcool.com/>. The online store exists in several language versions: Bulgarian, Bosnian, Croatian, Czech, Estonian, Greek, Hungarian, Italian, Latvian, Lithuanian, Polish, Romanian, Serbian, Slovenian and Slovak.

In its Privacy Policy, the controller states, quote: “FC ecom., With its registered office at Vellkomoravská 2866/9, Trenčín 911 05, IČO: 51 750 155, company registration number 36568 / R ("FACTCOOL" or "we") ensures the protection of personal data of its customers in accordance with the relevant legal provisions regarding data protection. This Privacy Policy describes how we collect, process and protect our Customers' personal data when browsing our Site and / or purchasing our Products.“ Similar is also provided in the Slovenian language version of the controller's Privacy Policy.

Since the controller has its single establishment in Slovak Republic, Slovak SA as LSA in this matter created Case register no. 102 666 in IMI system.

Slovak SA has requested FC ecom, s.r.o. in this matter for cooperation, in particular to indicate how the controller has dealt with the request of the data subject ([REDACTED] pursuant to Art. 15 of the GDPR and to provide an evidence to do so; whether the controller processes the personal data of the data subject and, if so, to what extent, for what purpose and on what legal basis the personal data are processed; what is the legal relationship between FC ecom, s.r.o. and Factcool Ltd. established in the United Kingdom regarding the processing of the personal data of the data subject ([REDACTED]

The controller answered, quote: „I'm sending you our written statement for this case with Mr. [REDACTED] We as FC Ecom s.r.o. have purchased brand name Factcool from company Factcool s.r.o. with their assets. We have no relations with Factcool ltd. and we did not shifted any personal data from any foreign country. Our company is solely based in Slovakia and we operate in several countries within Europe as an eshop, within our general terms and



conditions, where we clearly state who we are, where we are based and under which rules we operate. Every customer is asked to accept it prior to the purchase. We take GDPR very seriously and upon request, we delete all information about customers except information required by law about accounting for the Tax Office of Slovak Republic. Mr. [REDACTED] has contacted us with a request of providing him information about his personal data with reference to Factcool ltd. After we checked our database, we have informed Mr. [REDACTED] that we have no data available about him what so ever in our database, and therefore have nothing to delete + we have no relations to Factcool ltd. After we informed Mr. [REDACTED] about this situation and sincerely apologized for this IT error that might have occurred, through our external marketing partner, who had send newsletters for us in the past. He requested that we will compensate him financially or materially for misusing his information.“ The controller refused to compensate complainant financially or materially. The company in its statement states that complainant has not provided the controller with any proof of misuse; the controller never received even the mentioned Newsletter that he apparently received from the controller.

The controller has attached screenshots from its database, proving that the controller have no complainant's data stored and how the controller proceeds to customer requests for the removal of personal data from its database. The controller states that this case is most likely an IT error or complainant might have provided voluntarily his email address to one of the controller's partners at that time through marketing campaign, where upon entering his email address he might enter into competition to win certain prices and that way gave permission to use his e-mail address for marketing purposes of the controller's partners at that time. The controller states that he has none of complainant's personal data stored or available, which was proven by attached screenshots. The controller adds that every customer has an option to unsubscribe from any or all of its communications - newsletters includes – at the bottom of every email, or data subjects could contact the controller via telephone or e-mail to anonymise all given personal data.

Pursuant to Art 4 (7) GDPR, for the purposes of this Regulation: ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Pursuant to Art. 4 (23) GDPR, for the purposes of this Regulation: ‘cross-border processing’ means either:

- (a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
- (b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Pursuant to Art. 15 GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:



- (a) the purposes of the processing;
- (b) the categories of personal data concerned;
- (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (f) the right to lodge a complaint with a supervisory authority;
- (g) where the personal data are not collected from the data subject, any available information as to their source;
- (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Pursuant to Art 56 (1) GDPR, without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

Pursuant to Art 56 (2) GDPR, by derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

The purpose of personal data protection proceeding (hereafter as “proceeding”) is to determine whether there was any infringement of the rights of natural persons when their personal data were processed or if there was any violation to this Act or GDPR in the area of personal data protection; and, if any deficiencies are identified, if it is reasonable and useful, to impose corrective measures or impose a fine for violation of this Act or GDPR .

Pursuant to Sec. 100 (1) of the Slovak Data Protection Act, the proceeding is initiated based on the complaint of a data subject that claims that his or her rights lay down by this Act are directly influenced (hereafter as “the complainant”), or without a complaint.

Pursuant to Sec. 100 (5) (a) of the Slovak Data Protection Act, (5) The Office shall dismiss the complaint if the complaint is manifestly unfounded.

On the basis of abovementioned findings, the Slovak SA shall dismiss the complaint pursuant to Sec. 100 (5) (a) of the Slovak Data Protection Act, because during the investigation the controller had proved that the controller had no complainant's personal data stored in its database. The complainant had sent to the controller the Request for access pursuant to Art. 15 of the GDPR via e-mail [REDACTED] on August 19, 2019. The controller had replied from email address factcool-si@factcool.com on August 22, 2019 that Factcool s.r.o. (Slovakia) sold Factcool.com online store to FC ecom s.r.o. (Slovakia) and that Factcool s.r.o.



only sold goods in Slovakia. The controller explained to the complainant in this e-mail that in Slovenia (from where the complainant is), Factcool Ltd. from United Kingdom sold the Factcool.com online store. The controller wrote to the complainant that FC ecom s.r.o. (the controller) does not have any customer data from Factcool Ltd as Factcool Ltd own the data for Slovenian market. Pursuant to Art. 15 of the GDPR, the data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information in the letters a) to h) of the Art. 15. The controller had reacted to the complainant's request up to 3 days after complainant sent their request. On August 22, 2019 the controller confirmed to the complainant that FC ecom s.r.o. (the controller) does not have any customer data from Factcool Ltd as Factcool Ltd owns the data for Slovenian market, thus the access for information in the letters a) to h) is appeared to be objectively non-accessible in this case. The controller has fully cooperated with the Slovak SA and has attached screenshots from its database, proving that the controller has no complainant's personal data stored in its database and does not process any of complainant's personal data according to Art. 15 of the GDPR.

A complaint may be lodged against this decision within 15 days from the delivery of this decision pursuant to Slovak National Act no. 9/2010 Coll. on complaints. This does not affect the right to an effective judicial remedy against a legally binding decision of the supervisory authority pursuant to Art. 78 par. 1 GDPR.

- The complaint pursuant to Act no. 9/2010 Coll. must be in writing and can be submitted in paper or electronic form.
- The complaint pursuant to Act no. 9/2010 Coll. must contain the name, surname and address of the complainant. If the complaint is submitted by a legal entity, it must contain its name and registered office, name and surname of the person authorized to act on its behalf. The complaint in paper form must contain the complainant's handwritten signature. If it is possible to deliver documents to the complainant in accordance with this Act in electronic form, the complaint may also contain the complainant's address for such service.
- The complaint pursuant to Act no. 9/2010 Coll. must be legible and comprehensible. It must be clear from whom it is directed, what shortcomings it points out and what the complainant claims (hereinafter referred to as the "subject of the complaint").

Should new relevant facts be identified in a complaint lodge against this decision, the case could be reviewed in the personal data protection proceedings.

JUDr [REDACTED]
Head of the Department
of administrative proceedings
Office for Personal Data
Protection of the Slovak Republic



IMI FD 517446

521.14435

1. Summary of the case

On 11 August 2021 the representative of the complainant left a review of an accommodation on the platform of the data controller. The data controller operates an online travel marketplace platform. On 3 September 2021 the complainant noticed that the accommodation provider had replied to the review. In this reply the accommodation provider mentioned the full name of the complainants. On the same day the representative of the complainants updated the review and objected to the publication of the complainants' personal data. Also on 3 September 2021 the representative noticed that the reply of the accommodation provider was removed. On 4 September 2021 the representative contacted the data controller to complain about the accommodation provider. On 4 September 2021 the accommodation provider posted an updated reply to the review which, again, contained the full names of the complainants. The representative updated the review and pointed out that the names of the complainants should not be in the reply of the accommodation provider whilst referring to the data protection office of the data controller. The accommodation provider removed their reply on 6 September 2021 and posted an updated reply on 7 September 2021 without mentioning the names of the complainants.

The data controller sent an auto-reply to the representative on 4 September 2021 and another response on 1 October 2021. In this response the data controller informed the representative that they have noted the complaint with the accommodation. The data controller informed the representative that reviews are updated within 10 days and that they should not be able to see the review afterwards. On 2 October 2021 the representative responded to the e-mail of the data controller, explaining that the reply of the accommodation partner has changed multiple times in the meantime and that they do not understand what the data controller means by 'not being able to see the review. The updated review, without personal data, is still visible according to the complainant. The representative also stated a second issue, that they were concerned that the monitoring mechanism used by the data controller to prevent the publication of names on the platform does not seem to work considering that both the reply of 3 September 2021 and of 4 September 2021 did contain the names of the complainants. The complainants believe that there

is a systematic failure with regard to the publication of names of data subjects in the reviews on their platform.

On 19 August 2022 the responsible SA requested additional information regarding this complaint from the data controller, e.g. how they monitor the reviews. The data controller confirms that it has systems in place that screen for names used in reviews submitted by users of its platform. All review submissions are reviewed by automated systems, which are configured (and updated from time to time) to assess each post for possible non-conformance with data controllers' guidelines and policies. The guidelines include the rule that the accommodation provider's response to a review posted by a guest may not mention any personal information not voluntarily disclosed in the guest's review. These automated systems distinguish between posts that can be published and posts that require manual review by a dedicated team of the data controller.

In this specific case, the response was published while certain names were still visible. When this happens, the data controller's standard process is to promptly delete such posts when they are flagged, e.g. when a customer sends a related message to the data controller's customer service. In this specific case, the accommodation provider on its own initiative removed its post on 6 September after the data subject updated her review on 3 September 2021. The post of the accommodation provider was visible on the data controller's platform from 12 August 2021 until 6 September 2021. This means that the data subject's personal data in the accommodation provider's response was removed within 3 days after the data subject updated their review to complain about it.

In their response to the SA the data controller states, that the content moderating system is not flawless, and that this does not indicate that the measures taken by the data controller to ensure that accommodation providers do not share personal data in their replies are insufficient. If a submission passes the review while still containing personal information, the data subject can flag the submission and the data controller will delete the posts.

2. Legal assessment by the Lead Supervisory Authority

(Norm allegedly infringed: Articles 5, 6, 7, 12, 13, 14 and 17 GDPR)

The Lead Supervisory Authority investigated the case and came to the conclusion that further investigation would be required to gain a deeper understanding of the content moderating system and the exact steps and parameters. The supervisory authority finds such an investigation disproportionate with regard to this specific complaint, considering that the personal data of the complainant was removed within 3 days after the representative updated their review to complain about it. The SA deems this matter investigated to the extent appropriate and rejects the complaint in accordance with Article 60(8) GDPR.



Berlin Commissioner for Data Protection and Freedom of Information
Alt-Moabit 59-61, 10555 Berlin, Germany

IMI FD 517447

521.15203

1. Summary of the case

The complainant rented an accommodation through the online platform of the controller on 28 June 2020. On 29 June 2020 they received a message by the accommodation provider, in which they were requested to contact them through a specific email address. After having contacted this email address, they were informed that the controller had not updated the calendar for the booked accommodation and that renting the apartment was therefore no longer possible. After several email exchanges, the complainant decided to rent a comparable accommodation and paid the reservation to a Spanish bank account. Upon arrival, however, the complainant discovered that no such accommodation existed and that they had probably been victims of fraud. They thus suspected that a data leak occurred at the controller, through which the specific information used for the originally rented accommodation may have been leaked.

The Lead Supervisory Authority initiated a written hearing of the controller on 19 August 2022, in which it, among other things, inquired as to whether the company listed for the accommodation had been previously known for/or suspected of committing fraud. The controller confirmed this, and also informed that as part of standard procedure the reservation on the platform was cancelled. With regards to the specific reservation, the controller's systems indicated that the reservation had been cancelled by the complainant themselves. The cancellation was free of charge, resulting in no money being withdrawn from the credit card of the complainant. As the payment for the reservation had been carried out directly by the controller, the accommodation provider did not receive the payment data by the controller. An investigation has instead demonstrated that the suspected fraudulent accommodation provider had instead requested the person to answer directly to an email address provided by the

suspected fraudulent accommodation provider. The communication between the complainant and the suspected fraudulent accommodation provider was investigated by the responsible authority, which concluded that the complainant themselves had sent an email to the suspected fraudulent accommodation. By doing so, it is possible that the complainant had thus transmitted personal data directly to the suspected accommodation provider, potentially including details of his credit card. The controller clarified that this occurred outside of their platform and that such communication was not visible for the controller.

2. Legal assessment by the Lead Supervisory Authority

The Lead Supervisory Authority could not determine an infringement against Art. 32 Para. 1 GDPR by the controller. As a result of the complainant sending their data directly to the suspected fraudulent accommodation provider, the data of the complainant were not leaked through the platform provider. It was therefore also not possible to determine a failure of the employed technical and organisational measures by the controller in accordance with Art. 32 Para. 1 GDPR.

Summary Final Decision Art 60

Complaint

EDPBI:FR:OSS:D:2023:762

Violation identified ; Administrative fine

Background information

Date of final decision:	11 May 2023
Date of broadcast:	22 May 2023
LSA:	FR
CSAs:	All SAs
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 9 (Processing of special categories of personal data), Article 26 (Joint controllers), Article 32 (Security of processing)
Decision:	Violation identified, Administrative fine.
Key words:	Sensitive data, Health records Joint controllers Administrative fine, Anonymisation, Data retention, Data security

Summary of the Decision

Origin of the case

The controller is a website dedicated to health and wellness, established in France ("the company"). It mainly offers articles, tests, quizzes and discussion forums related to well-being and health. The company's website has visitors from all Member States of the European Union.

On 26 June 2020, the LSA received a complaint concerning all of the processing of personal data of users implemented by the controller on its website and, in particular, the legal ground for processing users' personal data when a user takes health-related tests; the provision of information to users of the website, as well as data security. The LSA carried out an online audit in September 2020, an on-site inspection in October 2020 and sent a request for information to the company.

Findings

Firstly, the LSA found that the controller has not sufficiently monitored the performance of the contractual instructions it gave to its processor and has not exercised satisfactory **control over the measures the processor implemented** to ensure GDPR compliance (in particular, the absence of collection of personal data or its anonymisation). The LSA considered that the retention of test data did not appear necessary after the communication of the test result to the user, finding a **breach of Article 5(1)(e) of the GDPR**. Until 11 October 2020, the responses to the tests and quizzes and the IP addresses of users were retained for 24 months from the time of completion of the tests. After 11 October 2020, the responses to the tests and quizzes were retained for a period of three months from the time of completion of the tests due to ineffective anonymisation, using the SHA256 function without a hash key. The LSA also found that the company retained user account's data for more than three years due to ineffective anonymisation as it retained the unique identifier ("id_user") of the user, associated with their pseudonymised username. According to the LSA, this process did not correspond to anonymisation but to a mere pseudonymisation. The LSA recalled that the pseudonymisation of personal data is a reversible operation and that it is possible to find a person's identity by having additional information. However, the LSA noted that the company complied during the procedure with the implementation of a new anonymisation procedure, so there was no need to send an injunction to the company on this point.

Secondly, as to the health-related tests, the LSA concluded that the data obtained when users take tests on the company's website amounts to personal data concerning health. In the absence of other lawful grounds that can be invoked to allow such processing under Article 9(2)(b) to (j) of the GDPR, the LSA considered that such processing can only be implemented based on the data subject's **explicit consent**. Consequently, the LSA considered that the company breached **Article 9 of the GDPR**. The LSA noted that the company brought this processing activity into compliance over the course of the procedure by introducing a consent checkbox.

Thirdly, regarding the **obligation to inform data subjects pursuant to Article 13 of the GDPR**, the LSA found no violation.

Fourthly, the LSA noted that the controller was jointly liable with an advertising company with regard to processing related to the marketing of advertising spaces on its website, and with another company for the processing using the technical tools and functional structures made available by the latter. The LSA concluded that the company **breached Article 26 of the GDPR** due to the absence of a joint processing agreement within the meaning of this article at the time of the LSA's audits.

Lastly, the LSA considered that the company **failed to implement the basic security measure** that constituted the use of the "HTTPS" protocol or another equivalent security measure. According to the LSA, this characterised a **breach of Article 32 of the GDPR**, as the security measures were not adequate to the risks to the protection of personal data (i.e. health data in this case). Similarly, the lack of security for the storing of users' passwords was also found to constitute a breach of this provision. The LSA noted the controller's subsequent compliance measures, nonetheless recalling that they cannot absolve the controller from its responsibility for past events.

Decision

The LSA noted all the infringements to Articles 5(1)(e), 9(2), 26 and 32 of the GDPR. Taking into account the company's liability, its financial capacity and the relevant criteria of Article 83 of the GDPR (e.g. the high number of people affected; the company's negligence, etc.), the LSA imposed an **administrative fine of 280,000 Euros** with regard to the GDPR breaches and an administrative fine of 100,000 euros (with regard to the breaches set out in Article 82 of the French Data Protection Act). The LSA also decided to publish the final decision on its website and on the Légifrance website for two years, after which the company will not be identifiable anymore.

Summary Final Decision Art 60

Complaint

Compliance order

EDPBI:FR:OSS:D:2022:330

Background information

Date of complaint:	19 August 2020
Date of final decision:	03 February 2022
LSA:	FR
CSAs:	AT, BE, BG, HR, CY, CZ, DK, EE, FI, DE, DEBW, DEBY, DEBE, DEHB, DEHH, DEHE, DEHI, DEMV, DENW, DERP, DESL, DESN, DEST, DESH, DESH, DETH, HU, IE, IT, LV, LI, LT, MT, NL, PL, PT, RO, SK, SI, ES, SE
Legal Reference(s):	Article 44 (General principle for transfers), Article 46 (Transfers by way of appropriate safeguards), Article 49 (Derogations for specific situations).
Decision:	Compliance order
Key words:	Consumer protection, Cookies, E-Commerce, International transfer, Online and electronic devices, Pseudonymisation.

Summary of the Decision

Origin of the case

The controller performs distance selling activity and is registered in France. On 12 October and 16 November 2020, the LSA delegation carried out a documentary audit by sending questionnaires to the controller. The questionnaires concerned the transfer of personal data of the visitors of the controller's French language version website to the United States of America. As a response to the LSA's questionnaires, the controller informed the LSA that it had decided to integrate the Google Analytics functionality on its website. The controller stated that the statistics obtained through Google Analytics concerned individuals in several member states of the EU. The controller considered that the processing activity resulting from the integration of Google Analytics appeared to meet the definition of cross-border processing as referred to in Article 4.23 b) of the GDPR. On 9 March 2021, the LSA sent a questionnaire to Google LLC covering the Google Analytics feature, to which Google LLC replied on 9 April 2021. In its reply, Google LLC stated that data collected on the controller's website through the Google Analytics functionality are stored in and thus transferred to the United States of America. In

accordance with Article 56 GDPR, on 5 August 2021, the LSA informed all the European supervisory authorities of its competence to act as lead supervisory authority. As part of the cooperation procedure based on Article 60 of the GDPR, a draft decision was submitted on 4 January 2022. The draft decision did not give rise to any relevant and reasoned objections.

Findings

Firstly, the LSA concluded that, by deciding to implement the Google Analytics feature on its website for the purposes of measuring its audience and the performance of its media campaigns, the company managing the website determined the means and purposes of the collection and processing of the data obtained through the use of Google Analytics. Thus, the company should be considered controller within the meaning of Art. 5(7) of the GDPR. Secondly, the LSA established that the data collected under the Google Analytics feature and transferred to the United States of America constituted personal data within the meaning of Art. 4 of the GDPR. Referring to Recital 30 of the GDPR, the LSA noted that online identifiers, such as IP addresses or information stored in cookies, can commonly be used to identify a user in particular when combined with other similar types of information. In the case at hand, the controller would, under the Google Analytics feature, process a visitor's identifier (the Google Analytics customer ID unique for each user), internal identifier by the controller (in case a visitor has logged into the website through a user account provided by the controller), order identifiers (if such existed) and IP addresses. As stated in Recital 26 of the GDPR, the singling out of individuals is sufficient to make individual website visitors identifiable. Finally, on the question of whether there was a breach of the obligation to regulate transfers of personal data outside the European Union, the LSA presented the following findings. According to Art. 44 of the GDPR, a transfer of personal data to a third country shall take place only if the conditions laid down in Chapter V of the GDPR are complied with by the controller and processor. The LSA pointed out that there is currently no adequacy decision as referred to in Art. 45 of the GDPR which the parties of the transfer can rely upon when transferring personal data to the USA. Moreover, pursuant to CJEU's judgement in case C-311/18, standard contractual clauses do not alone provide appropriate safeguards for a transfer of personal data to the USA as they are contractual in nature and therefore do not prevent US authorities from accessing the transferred data. With regard to the contractual, organisational and technical measures to supplement the standard data protection clauses implemented by Google LLC, the LSA found that none of the measures, such as the notification of users, publication of a transparency report, protection of communications between the Google services and encryption of data at rest in data centres, prevented or reduced the possibility of US authorities to access the data. Thus, the safeguards could not be deemed effective in the present case. Further, the derogations set forth in Art. 49 of the GDPR were not applicable as the data subjects had not given their explicit consent to the transfer within the meaning of Art. 49(1)(a) of the GDPR. The controller had not presented evidence to support its claim to base the transfer on Art. 49(1)(b) either. Based on the aforementioned, the LSA concluded that the controller could not invoke any of the tools provided for in Chapter V of the GDPR to justify the transfer of personal data of visitors to its website. Thus, it had undermined the level of protection of the personal data of data subjects as guaranteed in Art. 44 of the GDPR.

Decision

The controller was ordered to bring its data processing activity into compliance with Art. 44 of the GDPR notably by ceasing its processing activities under the Google Analytics functionality within one month of the notification of the LSA's decision and provide supporting documentation to the LSA confirming that it has complied with the aforementioned request within the abovementioned time limit.



PENALTY NOTICE

Section 155, Data Protection Act 2018

Case ref: COM0783542

**British Airways plc
Waterside
PO BOX 365
Harmondsworth
UB7 0GB**

16 October 2020

1. INTRODUCTION & SUMMARY

- 1.1. This Penalty Notice is given to British Airways plc ("BA") pursuant to section 155 and Schedule 16 to the Data Protection Act 2018 (the "DPA"). It relates to infringements of the General Data Protection Regulation (the "GDPR"), which came to the attention of the Information Commissioner ("the Commissioner") as a result of an incident that took place between 22 June and 5 September 2018.
- 1.2. In summary, between 22 June and 5 September 2018, a malicious actor ("the Attacker") gained access to an internal BA application through the use of compromised credentials for a Citrix remote access gateway ("CAG").

[REDACTED] After gaining access to the wider network, the Attacker traversed across the network. This culminated in the editing of a Javascript file on BA's website (www.britishairways.com). The edits made by the Attacker were designed to enable the exfiltration of cardholder data from the "britishairways.com" website to an external third-party domain (www.BAways.com) which was controlled by the Attacker. In this Penalty Notice, the events of 22 June to 5 September 2018 are referred to as "the Attack".

- 1.3. BA is a subsidiary of International Airlines Group, which is registered in Spain but has its operational headquarters in the United Kingdom. The data subjects affected by this breach were BA customers in the United Kingdom, in the EU, and in the rest of the world.
- 1.4. BA was the controller of the personal data of its customers, within the meaning of section 6 DPA and Article 4(7) GDPR, as it determined the purposes and means of the processing of the personal data. By, *inter alia*, collecting, recording, organising, structuring and storing the personal data of its customers, BA was processing that data within the meaning of section 3(4) DPA and Article 4(2) GDPR.
- 1.5. BA acted promptly in notifying the Commissioner of the Attack on 6 September 2018 and thereby complied with its obligations in this

respect. The Commissioner considers that BA has cooperated fully with her investigation and has taken that into account.

- 1.6. BA does not admit liability for breach of the GDPR. However, for the reasons set out in this Penalty Notice, the Commissioner has found that BA failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including: protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and by Article 32 GDPR.
- 1.7. The Commissioner has found that, in all the circumstances of the case and having regard to BA's representations and the matters listed in Article 83(1) and (2) GDPR, the infringements constitute a serious failure to comply with the GDPR and, accordingly, that the imposition of a penalty is appropriate. The amount of the penalty that the Commissioner has decided to impose, having taken into account a range of mitigating factors set out further below and the impact of the Covid-19 pandemic, is £20m.
- 1.8. Pursuant to Article 56 GDPR, the Commissioner is acting as lead supervisory authority in respect of the cross-border processing at issue in this case.

2. LEGAL FRAMEWORK

GDPR

- 2.1. On 25 May 2018, the GDPR entered into force, replacing the previous EU law data protection regime that applied under Directive 95/46/EC ("Data Protection Directive")¹. The GDPR seeks to harmonise the protection of fundamental rights in respect of personal data across EU Member States and, unlike the Data Protection Directive, is directly applicable in every Member State.²
- 2.2. The GDPR was developed and enacted in the context of challenges to the protection of personal data posed by, in particular:

¹ 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.

² Recital 3.

- a. the substantial increase in cross-border flows of personal data resulting from the functioning of the internal market;³ and
 - b. the rapid technological developments which have occurred during a period of globalisation.⁴ As Recital (6) explains: "... *The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities....*"
- 2.3. Such developments made it necessary for "*a strong and more coherent data protection framework 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...*".⁵
- 2.4. Against that background, the GDPR imposed more stringent duties on controllers and significantly increased the penalties that could be imposed for a breach of the obligations imposed on controllers (amongst others).⁶

The relevant obligations

- 2.5. Chapter 1 GDPR sets out the general provisions. Article 5 of Chapter II GDPR sets out the principles relating to the processing of personal data. Article 5(1) lists the six basic principles that controllers must comply with in processing personal data, including:

1. Personal data shall be:

...(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

- 2.6. Article 5(2) GDPR makes it clear that the "*controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')*".

³ Recital 5.

⁴ Recital 6.

⁵ Recital 7.

⁶ See, in particular, Recitals 11, 148, 150, and Article 5, Chapter IV and Article 83.

- 2.7. Chapter IV, Section 1 addresses the general obligations of controllers and processors. Article 24 sets out the responsibility of controllers for taking appropriate steps to ensure and be able to demonstrate that processing is compatible with the GDPR. Articles 28-29 make separate provision for the processing of data by processors, under the instructions of the controller.
- 2.8. Chapter IV, Section 2 addresses security of personal data. Article 32 GDPR provides:

1. Taking 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, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- (a) *the pseudonymisation and encryption of personal data;*
- (b) *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
- (c) ...
- (d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.*

2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- 2.9. Article 32 GDPR applies to both controllers and processors.

Penalties

- 2.10. Article 83(1) GDPR requires supervisory authorities to ensure that any penalty imposed in each individual case is “*effective, proportionate and dissuasive*”.
- 2.11. The principle that penalties ought to be effective, proportionate and dissuasive is a longstanding principle of EU law. The Commissioner

is under an EU law obligation to ensure that infringements of the GDPR are penalised in a manner that is effective, proportionate and dissuasive.

- 2.12. Further, Recital 148 emphasises, *inter alia*, that "in order to strengthen the enforcement of the rules of this Regulation, penalties including administrative fines should be imposed for any infringement of this Regulation, in addition to, or instead of appropriate measures imposed by the supervisory authority pursuant to this Regulation." It also records that due regard should be given to the:

... nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor...

- 2.13. Recital 150 provides as follows:

In order to strengthen and harmonise administrative penalties for infringements of this Regulation, each supervisory authority should have the power to impose administrative fines. This Regulation should indicate infringements and the upper limit and criteria for setting the related administrative fines, which should be determined by the competent supervisory authority in each individual case, taking into account all relevant circumstances of the specific situation, with due regard in particular to the nature, gravity and duration of the infringement and of its consequences and the measures taken to ensure compliance with the obligations under this Regulation and to prevent or mitigate the consequences of the infringement. Where administrative fines are imposed on an undertaking, an undertaking should be understood to be an undertaking in accordance with Articles 101 and 102 TFEU for those purposes. Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of

administrative fines. It should be for the Member States to determine whether and to which extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

- 2.14. In line with the above, when deciding whether to impose a fine and the appropriate amount of any such fine, Article 83(2) GDPR requires the Commissioner to have regard to the following matters:

- (a) *the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;*
- (b) *the intentional or negligent character of the infringement;*
- (c) *any action taken by the controller or processor to mitigate the damage suffered by data subjects;*
- (d) *the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;*
- (e) *any relevant previous infringements by the controller or processor;*
- (f) *the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;*
- (g) *the categories of personal data affected by the infringement;*
- (h) *the manner in which the infringement became known to the supervisory authority, including whether, and if so to what extent, the controller or processor notified the supervisory authority of the infringement;*
- (i) *where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;*

- (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
 - (k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses avoided, directly or indirectly from the infringement.⁷
- 2.15. Article 83(5) GDPR provides that infringements of the basic principles for processing imposed pursuant to Article 5 GDPR will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €20 million or, in the case of an undertaking, up to 4% of its total worldwide annual turnover of the preceding financial year, whichever is higher.
- 2.16. Article 83(4) GDPR provides, *inter alia*, that infringements of the obligations imposed by Article 32 GDPR on the controller and processor will, in accordance with Article 83(2) GDPR, be subject to administrative fines of up to €10 million or, in the case of an undertaking, up to 2% of its total worldwide annual turnover of the preceding financial year, whichever is higher.
- 2.17. Article 82(3) GDPR addresses the circumstances in which the same or linked processing operations give rise to infringements of several provisions of the GDPR. It provides that "... *the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement*".
- 2.18. Article 83(8) GDPR provides that the exercise by any supervisory authority of its powers to fine undertakings will be subject to procedural safeguards, including an effective judicial remedy and due process.
- Cooperation and consistency**
- 2.19. Where, as here, the processing in issue is cross-border, Article 56 GDPR makes provision for the designation of a lead supervisory authority. In this case, the Commissioner is acting as the lead

⁷ See also the Article 29 Data Protection Working Party *Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679*, adopted on 3 October 2017, endorsed by the European Data Protection Board at its first plenary session. These provide a high-level overview of the assessment criteria set out in Article 83(2) GDPR in Section III.

supervisory authority. Chapter VII GDPR establishes the regime for ensuring cooperation between lead and other concerned supervisory authorities, and permitting unified decision-making.⁸

2.20. Article 60 GDPR provides:

- 1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.*
- 2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.*
- 3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.*
- 4. Where any of the other supervisory authorities concerned within a period of four weeks after having been consulted in accordance with paragraph 3 of this Article, expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority shall, if it does not follow the relevant and reasoned objection or is of the opinion that the objection is not relevant or reasoned, submit the matter to the consistency mechanism referred to in Article 63.*
- 5. Where the lead supervisory authority intends to follow the relevant and reasoned objection made, it shall submit to the other supervisory authorities concerned a revised draft decision for their opinion. That revised draft decision shall be subject to the procedure referred to in paragraph 4 within a period of two weeks.*

⁸ The relevant provisions enacting this regime must be read subject to, in particular, Articles 7, 70 and 127-128 and 131 GDPR.

6. *Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.*
 7. *The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision.*
 8. *By derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.*
 9. *Where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint, a separate decision shall be adopted for each of those parts of the matter. The lead supervisory authority shall adopt the decision for the part concerning actions in relation to the controller, shall notify it to the main establishment or single establishment of the controller or processor on the territory of its Member State and shall inform the complainant thereof, while the supervisory authority of the complainant shall adopt the decision for the part concerning dismissal or rejection of that complaint, and shall notify it to that complainant and shall inform the controller or processor thereof.*
 10. *After being notified of the decision of the lead supervisory authority pursuant to paragraphs 7 and 9, the controller or processor shall take the necessary measures to ensure compliance with the decision as regards processing activities in the context of all its establishments in the Union. The controller or processor shall notify the measures taken for complying with the decision to the lead supervisory authority, which shall inform the other supervisory authorities concerned. ...*
- 2.21. Article 60(4) refers to the consistency mechanism, which is in Section 2 of Chapter VII GDPR. Article 63 provides that: "In order

to contribute to the consistent application of this Regulation throughout the Union, the supervisory authorities shall cooperate with each other and, where relevant, with the Commission, through the consistency mechanism as set out in this Section.” Article 65 GDPR provides, insofar as relevant, that:

Dispute resolution by the Board

1. In order to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases:

(a) where, in a case referred to in Article 60(4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. The binding decision shall concern all the matters which are the subject

2. The decision referred to in paragraph 1 shall be adopted within one month from the referral of the subject-matter by a two-thirds majority of the members of the Board. That period may be extended by a further month on account of the complexity of the subject-matter. The decision referred to in paragraph 1 shall be reasoned and addressed to the lead supervisory authority and all the supervisory authorities concerned and binding on them.

3. Where the Board has been unable to adopt a decision within the periods referred to in paragraph 2, it shall adopt its decision within two weeks following the expiration of the second month referred to in paragraph 2 by a simple majority of the members of the Board. Where the members of the Board are split, the decision shall be adopted by the vote of its Chair.

4. The supervisory authorities concerned shall not adopt a decision on the subject matter submitted to the Board under paragraph 1 during the periods referred to in paragraphs 2 and 3.

5. The Chair of the Board shall notify, without undue delay, the decision referred to in paragraph 1 to the supervisory authorities concerned. It shall inform the Commission thereof. The decision shall be published on the website of the

Board without delay after the supervisory authority has notified the final decision referred to in paragraph 6.

6. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged shall adopt its final decision on the basis of the decision referred to in paragraph 1 of this Article, without undue delay and at the latest by one month after the Board has notified its decision. The lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged, shall inform the Board of the date when its final decision is notified respectively to the controller or the processor and to the data subject. The final decision of the supervisory authorities concerned shall be adopted under the terms of Article 60(7), (8) and (9). The final decision shall refer to the decision referred to in paragraph 1 of this Article and shall specify that the decision referred to in that paragraph will be published on the website of the Board in accordance with paragraph 5 of this Article. The final decision shall attach the decision referred to in paragraph 1 of this Article.

DPA

The Commissioner

- 2.23. Section 115 DPA establishes that the Commissioner is the UK's supervisory authority for the purposes of the GDPR. Section 115 DPA provides, *inter alia*, that the Commissioner's powers under Articles 58(2)(i) (the power to impose administrative fines) and 83 GDPR are exercisable only by giving a penalty notice under section 155 DPA.

Penalties

- 2.24. Section 155(1) DPA provides that, if the Commissioner is satisfied that a person has failed or is failing as described in section 149(2) DPA, the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice.
- 2.25. Section 149(2) DPA provides:

(1) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following –

- (a) *a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);*
 - (b) ...
 - (c) *a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors)...*
- 2.26. Section 155 DPA sets out the matters to which the Commissioner must have regard when deciding whether to issue a penalty notice and when determining the amount of the penalty.
- 2.27. Section 155(2) DPA provides that, subject to subsection (4), when deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commissioner must have regard to the matters listed in Article 83(1) and (2) GDPR.
- 2.28. Schedule 16 includes provisions relevant to the imposition of penalties. Paragraph 2 makes provision for the issuing of notices of intent to impose a penalty, as follows:
- (1) *Before giving a person a penalty notice, the Commissioner must, by written notice (a "notice of intent") inform the person that the Commissioner intends to give a penalty notice.*
 - (2) *The Commissioner may not give a penalty notice to a person in reliance on a notice of intent after the end of the period of 6 months beginning when the notice of intent is given, subject to sub-paragraph (3).*
 - (3) *The period for giving a penalty notice to a person may be extended by agreement between the Commissioner and the person.*
- 2.29. Paragraph 5 sets out the required contents of a penalty notice, in accordance with which this Penalty Notice has been prepared.
- Guidance
- 2.30. Section 160 DPA requires the Commissioner to produce and publish guidance about how she intends to exercise her functions. With respect to penalty notices, such guidance is required to include:

- (a) provision about the circumstances in which the Commissioner would consider it appropriate to issue a penalty notice;
 - (b) provision about the circumstances in which the Commissioner would consider it appropriate to allow a person to make oral representations about the Commissioner's intention to give the person a penalty notice;
 - (c) provision explaining how the Commissioner will determine the amount of penalties;
 - (d) provision about how the Commissioner will determine how to proceed if a person does not comply with a penalty notice.
- 2.31. Pursuant to section 161 DPA, the Commissioner's first guidance documents issued under section 160(1) DPA had to be consulted upon and laid before Parliament by the Secretary of State in accordance with the procedure set out in that section. Thereafter, in issuing any altered or replacement guidance, the Commissioner is required to consult the Secretary of State and such other persons as she considers appropriate. The Commissioner must also arrange for such guidance to be laid before Parliament.

The Commissioner's Regulatory Action Policy

- 2.32. On 4 May 2018, the Commissioner opened a consultation process on how the Commissioner planned to discharge her regulatory powers under the DPA. The consultation attracted responses from across civil society, commentators, and industry (including the finance and insurance, online technology and telecoms, and charity sectors). The consultation ended on 28 June 2018. Having taken all the views received during the consultation process into account, the Regulatory Action Policy (the "**RAP**") was submitted to the Secretary of State and laid before Parliament for approval.
- 2.33. Pursuant to section 160(1) DPA, the Commissioner published her RAP on 7 November 2018. Under the heading "Aims", the RAP explains that it seeks to:
 - "Set out the nature of the Commissioner's various powers in one place and to be clear and consistent about when and how we use them";

- “*Ensure that we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals’ information rights are properly protected*”;
 - “*Guide the Commissioner and our staff in ensuring that any regulatory action is targeted, proportionate and effective...⁹*”
- 2.34. The objectives of regulatory action are set out at page 6 of the RAP, including:
- “*To respond swiftly and effectively to breaches of legislation which fall within the ICO’s remit, focussing on [inter alia] those adversely affecting large groups of individuals*”.
 - “*To be effective, proportionate, dissuasive and consistent in our application of sanctions*”, targeting action taken pursuant to the Commissioner’s most significant powers on, *inter alia*, “*organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data*”.
- 2.35. The RAP explains that the Commissioner will adopt a selective approach to regulatory action.¹⁰ When deciding whether and how to respond to breaches of information rights obligations she will consider criteria which include the following:
- “*the nature and seriousness of the breach or potential breach*”;
 - “*where relevant, the categories of personal data affected (including whether any special categories of personal data are involved) and the level of any privacy intrusion*”;
 - “*the number of individuals affected, the extent of any exposure to physical, financial or psychological harm, and, where it is an issue, the degree of intrusion into their privacy*”;
 - “*whether the issue raises new or repeated issues, or concerns that technological security measures are not protecting the personal data*”;

⁹ RAP, page 5.

¹⁰ RAP, pages 6-7 and 10.

- “*the cost of measures to mitigate any risk, issue or harm*”;
 - “*the public interest in regulatory action being taken (for example, to provide an effective deterrent against future breaches or clarify or test an issue in dispute)*”.¹¹
- 2.36. The RAP explains that, as a general principle, “*more serious, high-impact, intentional, wilful, neglectful or repeated breaches can expect stronger regulatory action*”.¹²
- 2.37. Pages 24-25 of the RAP identify the circumstances in which the issuing of a Penalty Notice will be appropriate. They explain, *inter alia*, that in “*... considering the degree of harm or damage we may consider that, where there is a lower level of impact across a large number of individuals, the totality of that damage or harm may be substantial, and may require a sanction.*” The RAP stresses that each case will be assessed objectively on its own merits. However, it explains that, in accordance with the Commissioner’s risk-based approach, a penalty is more likely to be imposed in, *inter alia*, the following situations:
- “*a number of individuals have been affected*”;
 - “*there has been a degree of damage or harm (which may include distress and/or embarrassment)*”; and
 - “*there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it)*”.
- 2.38. The process the Commissioner will follow in deciding the appropriate amount of penalty to be imposed is described from page 27 onwards. In particular, the RAP sets out the following five-step process:
- a. **Step 1.** An ‘initial element’ removing any financial gain from the breach.

¹¹ RAP, pages 10-11.

¹² RAP, page 12.

- b. **Step 2.** Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at section 155(2)-(4) DPA.
- c. **Step 3.** Adding in an element to reflect any aggravating factors. A list of aggravating factors which the Commissioner would take into account, where relevant, is provided at page 11 of the RAP. This list is intended to be indicative, not exhaustive.
- d. **Step 4.** Adding in an amount for deterrent effect to others.
- e. **Step 5.** Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship). A list of mitigating factors which the Commissioner would take into account, where relevant, is provided at page 11-12 of the RAP. This list is intended to be indicative, not exhaustive.

3. CIRCUMSTANCES OF THE FAILURE: FACTS

The Attack

- 3.1. This section summarises the circumstances of the failures which are the subject of this draft decision. This summary does not seek to provide an exhaustive account of the technical detail involved in each step of the Attack.
- 3.2. During the course of her investigation, the Commissioner has considered detailed technical reports and information provided by BA, not all of which can be reproduced here. In addition:
 - a. on 5 September 2019 BA provided written representations in response to the Notice of Intent issued by the Commissioner on 4 July 2019 ("**BA's First Representations**"), which included new information relating to BA's understanding of the facts underlying the incident. The Commissioner's Notice of Intent is referred to as the "**NOI**";
 - b. on 11 October 2019 BA provided further information in response to requests for clarification from the Commissioner;

- c. on 5 December 2019 BA provided further information in response to a request for further clarification from the Commissioner; and
 - d. on 31 January 2020, BA provided further detailed written representations in response to the draft notice provided by the Commissioner on 23 December 2019 ("**BA's Second Representations**"), which provided further information about the incident.
- 3.3. What follows is a summary of the key stages of the Attack, which disclosed the inadequacies in BA's security measures.

Step 1: Initial access

- 3.4. On 22 June 2018, an individual or individuals (who have not to date been identified), and who are referred to in this Penalty Notice as the Attacker for ease of reference, gained access to BA's IT systems. The Attacker maintained the ability to access BA's systems undetected between 22 June and 5 September 2018.
- 3.5. The Attacker obtained access to BA's network via the CAG. CAG is a tool that allows users to access a network and applications whilst working remotely. BA's CAG provided access to some of its IT applications so that authorised BA users could remotely log-in and use those applications as if they were in their office.
- 3.6. The Attack began with the Attacker obtaining access to login credentials that BA had provided for the use of an employee of "Swissport", a third-party provider of cargo services to BA. BA has been unable to determine how the Attacker was able to obtain compromised login credentials of a Swissport employee based in Trinidad and Tobago, although BA has identified that the Attacker compromised five accounts connected to Swissport.
- 3.7. The CAG was configured to allow access to a specific application on BA's system via the use of a single username and password. The compromised Swissport account was not protected by the use of multi-factor authentication ("**MFA**") (MFA is a system that restricts access to systems to those that can complete a combination of two or more steps. This usually involves the individual having knowledge of a password and possession of a mobile device to which a code is

sent. This code must be input, as well as the password, before access is granted.) Since the Attack, BA has implemented MFA on all remote access accounts.

- 3.8. By utilising the login credentials of the compromised Swissport account, the Attacker was able to access a set of applications available for Swissport employees in connection with Swissport's provision of services to BA. [REDACTED]

[REDACTED] As explained below, the Attacker was then also able to access other parts of BA's network, beyond the access which BA intended to grant to Swissport employees.

Step 2: Breaking out of Citrix

- 3.9. Having obtained initial access to BA's network, the Attacker was able to 'break out' of the Citrix environment to gain access to parts of BA's network that BA did not intend to be accessed by Swissport employees.

- 3.10. BA's experts hypothesised that the Attacker was able to break out of the Citrix environment into BA's wider network by [REDACTED]

[REDACTED] However, BA's First Representations provided an alternative explanation based on new information.

- 3.11. BA now believes that [REDACTED]

[REDACTED] BA has said that it has not been able to establish conclusively how the Attacker was able to break out of the Citrix environment, but believes that the Attacker may have [REDACTED]

BA has since extended its Group Policy to restrict access [REDACTED]

- 3.12. [REDACTED]
- 3.13. [REDACTED]

- 3.14. BA believes that [REDACTED] allowed the Attacker to launch tools and scripts that Citrix would ordinarily have blocked, and to bring in tools from outside the Citrix environment. Having successfully copied a number of tools into the Citrix environment from outside the network, the Attacker used these tools to conduct network reconnaissance.

Step 3: Privilege escalation

- 3.15. During that reconnaissance, the Attacker obtained access to a file containing the username and password of a privileged domain administrator account [REDACTED] [REDACTED]. The login details were stored in plain text, in a folder on the server [REDACTED] [REDACTED]. In theory, any user within the relevant domain would therefore have had sufficient access to be able to open the file and obtain the domain administrator username and password.
- 3.16. A domain administrator account grants privileged access. In fact, it is an account which grants amongst the most privileged access of any user account in the Windows domain. Access to such domain administrator credentials therefore gave the Attacker virtually unrestricted access to the relevant compromised domain.¹³ Due to

¹³ The Commissioner has taken into account para 3.2 of BA's Second Representations.

the security risks that arise from the granting of such privileged access, the monitoring of these domain administrator accounts is a vital element of a system's security.¹⁴

Step 4:

- 3.17. On 26 June 2018, after gaining credentials for [REDACTED]
[REDACTED], the
Attacker was able to find a database System Administrator
username and password [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Step 5:

Step 6:

- 3.19.

¹⁴ See: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory> and <https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/active-directory-accounts>. See further the discussion in Section 6 below.

15

¹⁶ See para 3.5 of BA's Second Representations. We note that it is not accepted to be necessary for the Commissioner to set out this level of technical detail of each step of the Attack in this document.



Step 7: Personal data breach; XML file

- 3.20. By this stage the Attacker was in a position within the network where they had [REDACTED]
[REDACTED]
[REDACTED]
- 3.21. The Attacker then began to log in to different servers, presumably to find out what data was useful or valuable. On 26 July 2018, the Attacker was able to access log files, in plaintext, containing payment card details for BA redemption transactions.
- 3.22. The logging and storing of these card details (including, in most cases, CVV numbers) was not an intended design feature of BA's systems and was not required for any particular business purpose. It was a testing feature that was only intended to operate when the systems were not live, but which was left activated when the systems went live. BA has explained that this card data was being stored in plaintext (as opposed to in encrypted form) as a result of human error. This error meant that the system had been unnecessarily logging payment card details since December 2015. The impact of this failure was mitigated to some extent by the fact that the retention period of the logs was 95 days, which meant that the only accessible card details were those logged within the preceding 95 days. Nevertheless, the details of approximately 108,000 payment cards were potentially available to the Attacker.
- 3.23. BA informed the ICO that, around this time, the Attacker began to [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹⁷ BA's Second Representations, para 3.6. and BA's letter to the Commissioner, dated 11 October 2019.

Step 8: Personal data breach; payment card data [REDACTED]

- 3.24. During searches of BA's systems, the Attacker was able to identify files which contained code for the BA website. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- 3.25. Between 14 August 2018 and 25 August 2018, the Attacker [REDACTED] to redirect customer payment card data to a different website: "BAways.com". BAways.com was a site owned and controlled by the Attacker. It appears from BA's Second Representations that [REDACTED]
[REDACTED]
[REDACTED] had the effect of copying and redirecting payment card data to "BAways.com" (which BA refers to as "skimming").¹⁹ [REDACTED] remained active on BA's website for a period of 15 days between 21 August 2018 and 5 September 2018. During this time, when customers entered payment card information into BA's website, a copy was sent to the Attacker, without interrupting the normal BA booking and payment procedure.

Discovery and reporting of the breach

- 3.26. On 5 September 2018, a third party informed BA that data was being sent from britishairways.com to BAways.com.²⁰ Within 90 minutes,

¹⁸ BA's Second Representations, para 3.7.

¹⁹ *Ibid.*

²⁰ In its Second Representations, BA states that this is not correct: "[the third party] only notified BA that it has identified POST requests to the domain BAways.com". However, on 1 November 2018 provided the Commissioner with a document entitled "British Airways Data Incident: timeline of key events" which states: "...notification received from [the third party] advising of [confidential] data being sent to BAways.com". As POST requests are one element of data sharing between websites, the Commissioner does not consider this paragraph to be incorrect.

BA had adapted the malicious code and contained the vulnerability. 20 minutes later, BA blocked the URL paths to BAways.com.

- 3.27. The following day, 6 September 2018, BA notified the Commissioner, acquirer banks and payment schemes, and 496,636 affected customers about the incident. On 7 September 2018, BA notified an additional 39,480 affected customers.
- 3.28. BA has determined that 5 September 2018 is the last known date of unauthorised access to personal data within its system because that is the date on which it contained the vulnerability in its system and blocked the relevant URL paths.²¹
- 3.29. After 5 September 2018, BA implemented additional technical measures, including a next-generation anti-virus and endpoint detection and response tool, called "Crowdstrike Falcon".

4. PERSONAL DATA INVOLVED IN THE FAILURE

- 4.1. The Attacker is believed to have potentially accessed the personal data of approximately 429,612 individuals, in particular:
 - Name, address, card number and CVV number of BA customers - 244,000 data subjects;
 - Card number and CVV only – 77,000 data subjects;
 - Card number only – 108,000 data subjects;
 - Usernames and passwords of BA employee and administrator accounts; and
 - Usernames and pin numbers of up to 612 BA Executive Club accounts.²².

5. PROCEDURE

- 5.1. This section summarises the procedural steps the Commissioner has taken. In the Annex to this Penalty Notice, a more detailed chronology is provided.

²¹ See, for example, BA's Second Representations, paras 3.10-3.11; and BA's First Written Representations, paras 3.15-3.19.

²² These accounts had their passwords changed and were checked for fraudulent activity.

- 5.2. BA notified the Commissioner of the Attack on 6 September 2018. In response, the Commissioner commenced an investigation into the incident. That investigation included various exchanges with BA and considering detailed submissions and evidence.
- 5.3. On 4 July 2019 the Commissioner issued BA with the NOI, indicating an intention to impose a penalty, pursuant to section 155(1) and Schedule 16 DPA. The proposed penalty was £183.39m.
- 5.4. BA submitted written representations and provided further information in response to the NOI on 5 September 2019 (BA's First Representations). BA did not request an opportunity to make oral submissions.
- 5.5. On 4 October 2019, the Commissioner asked BA a number of technical clarification questions as a result of, in particular, the provision of new information in BA's First Representations about how the Attack occurred. BA responded to these questions and provided further information on 11 October 2019 and 18 October 2019. The Commissioner asked further technical clarification questions on 25 November 2019, which BA responded to on 5 December 2019.
- 5.6. Between July and November 2019, BA and the Commissioner exchanged correspondence about a number of issues, including: (a) whether, and if so when, the Commissioner would be convening the panel of technical advisers ("the **Panel**"); (b) the application of the Commissioner's Draft Internal Procedure, which is discussed further below; (c) the application and/or operation of the Article 60 GDPR consultation process; and (d) BA's request for further opportunities to make submissions or representations prior to and during the Article 60 GDPR process.
- 5.7. In a letter dated 6 December 2019, the Commissioner:
 - a. confirmed that she no longer intended to exercise her discretion to convene the Panel;
 - b. confirmed that the Draft Internal Procedure would not be taken into account in setting any penalty imposed on BA, having considered the detailed representations BA had made on this issue in its First Representations. The letter confirmed that the Commissioner would continue to apply the EU and domestic

- legislative framework in conjunction with the Regulatory Action Policy;
- c. outlined how the Article 60 consultation process would be conducted in this case; and
 - d. agreed to give BA the opportunity to make further representations on the Commissioner's draft decision if BA agreed to extend the six-month period for the issuing of a penalty notice prescribed in paragraph 2 of Schedule 16, paragraph 2 DPA. The Commissioner proposed a new deadline of 31 March 2020.
- 5.8. The Commissioner's position on these issues was informed, in particular, by careful consideration of BA's First Representations, including new factual information provided by BA. Given the length and detail of those representations, the need for further information, and the overall complexity of the case, that consideration took time and considerable resources. That process also resulted in changes and clarifications to the form and content of the draft decision.
- 5.9. The Commissioner is also especially mindful of the fact that she is acting as lead supervisory authority pursuant to Article 60 GDPR, and that it is important that her investigation and decision be as comprehensive as possible, since the draft decision must be submitted for the consideration of other supervisory authorities pursuant to Article 60(3).
- 5.10. Although the Commissioner considered that a further opportunity for detailed representations from BA was not required by law, the Commissioner decided to accede to BA's request having regard, in particular, to: (i) the complexity of the case, (ii) BA's representations, and (iii) the fact that this is one of the first major decisions made under the new EU data protection regime. In those circumstances, the Commissioner considered that a further opportunity to make representations was appropriate provided that an agreement could be reached on extending the statutory timetable for the issuing of the decision.
- 5.11. Following further correspondence, BA confirmed on 23 December 2019 its agreement to a statutory extension of time to 31 March

2020. On the same date, the Commissioner provided BA with a draft decision, inviting BA to make further written representations and to provide any other relevant evidence it wished the Commissioner to take into account.

- 5.12. On 31 January 2020, BA provided further detailed written representations on the Commissioner's draft decision (BA's Second Representations).
- 5.13. On 10 February 2020, the Commissioner wrote to BA with four follow-up questions, which arose from her consideration of the Second Representations, to which BA responded on 24 February 2020.
- 5.14. On 3 April 2020, the Commissioner wrote to BA requesting information regarding the impact of the Covid-19 pandemic on BA's financial position. This letter identified certain financial metrics which the Commissioner suggested were relevant to considering the financial impact of Covid-19 on BA.
- 5.15. On 12 May 2020, BA provided detailed representations on the impact of Covid-19 on its financial position ("the **Third Representations**").
- 5.16. Having considered BA's representations, on 12 June 2020 the Commissioner wrote to BA requesting further information on BA's financial position, and reiterated her request for the specific financial metrics set out in the correspondence of 3 April 2020. The Commissioner requested a response by 19 June 2020.
- 5.17. On 16 June 2020, BA requested an extension until 26 June 2020 and requested an opportunity to make submissions and share financial information via a video call. BA subsequently provided the further information on 22 June 2020 and made oral submissions by video call on 2 July 2020.
- 5.18. In light of the ongoing exchanges and the circumstances of the Covid-19 pandemic, BA and the Commissioner agreed to a series of further extensions of the statutory deadline to 30 September 2020.

6. CIRCUMSTANCES OF THE FAILURE: BREACHES

BA's failures

- 6.1. The Commissioner's conclusion is that between 25 May 2018, when the GDPR entered into force, and (at least) 5 September 2018, when BA took action to prevent the transfer of personal data to BAways.com, BA failed to comply with its obligations under Article 5(1)(f) and Article 32 GDPR. BA failed to process personal data in a manner that ensured appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures as required by Article 5(1)(f) and Article 32 GDPR.
- 6.2. This section describes the failures to comply with the GDPR that the Commissioner has identified and responds, where relevant, to BA's First and Second Representations and correspondence in relation to the Commissioner's NOI and draft decision.

The relevant standard

- 6.3. As set out above, Article 5 GDPR requires that personal data shall be processed in a manner which ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. The controller, in this case BA, is responsible for, and must be able to demonstrate compliance with, that requirement.
- 6.4. Article 32 GDPR concerns the security of processing personal data and, taking 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, requires a controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. Such measures may include encryption of personal data and a process for regularly testing, assessing and evaluating the effectiveness of such technical and organisational measures.²³

²³ See also Recitals 76, 77 and 83 GDPR.

- 6.5. Not every instance of unauthorised processing or breach of security will amount to a breach of Article 5 or Article 32. The obligation under Article 5 GDPR is to ensure *appropriate* security; the obligation under Article 32 is to implement *appropriate* technical and organisational measures to ensure an *appropriate* level of security, taking account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk to the rights of data subjects.
- 6.6. When considering whether there has been a breach of the GDPR and whether to impose a penalty, the Commissioner must avoid reasoning purely with the benefit of hindsight. The focus should be on the adequacy and appropriateness of the measures implemented by the data controller, risks that were known or could reasonably have been identified or foreseen, and appropriate measures falling within Article 5 and/or Article 32 GDPR that were not, but could and should have been, in place.²⁴
- 6.7. BA has confirmed that it agrees with the description given in paras 6.4-6.5 above regarding the factors to be taken into account to determine an appropriate level of security.²⁵ Its position remains, however, that the Commissioner has mis-applied the requirements of Articles 5(1)(f) and 32 GDPR. Its submissions in this regard are addressed below.
- 6.8. Overall, having carefully examined the available evidence, including the material provided: (a) in particular, written submissions provided prior to the issue of the NOI; and (b) BA's First and Second Representations and relevant correspondence, the Commissioner is satisfied that BA failed to put in place appropriate technical or organisational measures to protect the personal data being processed on its systems, as required by the GDPR.
- 6.9. The principal failures, which are the basis of the Commissioner's decision to impose a penalty, are identified below, by reference to Steps 1-8 of the Attack, described in section 3 above.

²⁴ At paragraph 3.15 of BA's Second Representations, BA accepts that paragraphs 6.2, 6.4 and 6.5 correctly set out the approach the Commissioner must adopt in this case.

²⁵ BA's Second Representations, para 3.15.

Step 1: Initial access

- 6.10. As set out above, initial access was gained to BA's network using the compromised credentials of a user within a third-party supplier to BA, who was accessing BA's network remotely. This is known as a "supply chain attack". There was, before the introduction of the GDPR, guidance in the public domain about the steps that organisations need to take to address the threat of such an attack.
- 6.11. For example, the Centre for the Protection of National Infrastructure published a Good Practice Guide in April 2015 entitled "*Mitigating Security Risk in the National Infrastructure Supply Chain*", which recommended that organisations view supply chain security risk as being an extension of existing arrangements to mitigate security risks within the organisation. Thus, organisations should have a Security Risk Implementation Plan in place, which includes the following:
 - risk scoring contracts to link in with existing risk assessments;
 - due diligence / accreditation / assurance of existing suppliers and the adoption, through contracts, of proportionate and appropriate measures designed to mitigate risk;
 - audit arrangements and compliance monitoring;
 - comprehensive mapping of all tiers of the upstream and downstream supply chains to the level of individual contracts; and
 - contract exit arrangements.
- 6.12. This advice has also been supplemented by more recent advice published by the National Cyber Security Council in January 2018.²⁶
- 6.13. On 9 April 2018, the Commissioner published guidance on *GDPR Security Outcomes*.²⁷ This document provides guidance to

²⁶ <https://www.ncsc.gov.uk/collection/supply-chain-security>

²⁷ <https://ico.org.uk/for-organisations/security-outcomes/>. The Commissioner accepts paras 3.23-3.24 of BA's Second Representations which states that these documents are not "*prescriptive requirements*".

organisations on how to put in place appropriate technical and organisational measures, as required by Articles 5(1)(f) and 32 GDPR. It explains that what constitutes "appropriate" measures will "*depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.*" Addressing specifically the risks posed by granting third parties / processors access to systems, it explains:

A.4 Data processors and the supply chain

[...] understand and manage security risks to your processing operations that may arise as a result of using third parties such as data processors. This includes ensuring that they employ appropriate security measures.

In the case of data processors, you are required to choose those that provide sufficient guarantees about their technical and organisational measures. The GDPR includes provisions where processors are used, including specific stipulations that must feature in your contract.

- 6.14. The guidance also refers and links to the NCSC's Supply Chain Security guidance document, referred to above. In relation to the issue of identity and access control, the Commissioner's guidance states: "*You should appropriately authenticate and authorise users (or any automated functions) that can access personal data. You should strongly authenticate users who have privileged access and consider two-factor or hardware authentication measures.*"
- 6.15. There has also been other guidance in the public domain for some time concerning identity access management standards, including the need to ensure that users only have access to software required for their role. For example, OWASP published a list of "Top Ten Proactive Controls 2016", which is described as a "*list of security concepts that should be included in every software development project*". Control number 6 is the implementation of appropriate access controls, which includes compliance with the principle of least privilege. That privilege is described as follows: "*when designing access controls, each user or system component should be allocated*

the minimum privilege required to perform an action for the minimum amount of time.”²⁸

- 6.16. The National Institute for Standards and Technology (“NIST”) in guidance entitled “Back to Basics: multi-factor authentication” (2016) explained that: “*you should use MFA whenever possible, especially when it comes to your most sensitive data...*”. This is consistent with later guidance published by the NCSC.²⁹
- 6.17. There are a number of appropriate measures that BA could have considered to mitigate the risk of an attacker being able to access the BA network by compromising a single username and password. These measures include, for example, MFA, external public IP address whitelisting, and IPSec VPN. Any one of these options would, in the Commissioner’s view, have been appropriate.
- 6.18. In the first instance, it is for the controller to consider what measures are appropriate for securing its system. BA’s own Network Access Control Policy of 7 October 2017 states: “*Multi-factor authentication shall be incorporated for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the network.*” It therefore appears that BA itself considered MFA to be an appropriate measure to mitigate the risk of unauthorised remote access via Citrix in the context of its network.
- 6.19. BA’s First Representations indicated that, [REDACTED]
[REDACTED]
[REDACTED]
³⁰
- 6.20. BA also confirmed to the Commissioner in its response to an Information Notice dated 12 October 2018 that it hosted 243 applications on the Citrix Access Gateway. Of these applications, 13 were not protected by MFA, [REDACTED].
- 6.21. BA has not provided a satisfactory explanation as to why Citrix access was the subject of a separate risk assessment process or why

²⁸ See: https://wiki.owasp.org/index.php/OWASP_Proactive_Controls_2016#6:_Implement_Access_Controls

²⁹ <https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services>

³⁰ BA’s First Representations, para 2.28.

it was deemed unnecessary for certain applications, [REDACTED], to comply with the policy requiring MFA.

- 6.22. BA has indicated that ■

³¹ However, BA has been unable to provide a copy of that document and, accordingly, the Commissioner has not been able to assess its contents as part of her consideration of whether BA had appropriate measures in place during the relevant period. It is unlikely, moreover, that [REDACTED] [REDACTED] would accurately reflect the full range of cyber security risks in 2018. Further, [REDACTED] before the enactment of the GDPR in 2016 and its coming into force in May 2018.

- 6.23. The use of MFA in accordance with BA's own policy, and which BA has since implemented across all remote access users, would have been an appropriate technical measure to implement for users remotely accessing [REDACTED].

6.24. In a letter dated 11 October 2019, BA responded to the Commissioner's queries³² about its use of MFA as follows:

³¹ Letter from BA to Commissioner of 11 October 2019.

³² BA's First Representations, paras 2.30-2.31.

- 6.25. This suggests that BA did not approach its obligations under Articles 5(1)(f) and 32 GDPR correctly. [REDACTED]
- [REDACTED]

[REDACTED] Even if BA did not wish to rely upon MFA to secure its remote access for the administrative reasons it has outlined, an alternative option would have been a VPN tool which operated between IP addresses (for example, an IPSEC VPN). Such a tool allows remote sites to be connected together in a manner that could have prevented the Attacker from using compromised third-party credentials.³³

- 6.26. In its Second Representations, BA claims that since [REDACTED] did not allow access to personal data, the fact that it was not protected by MFA is consistent with relevant guidance. However, in practice BA's position is that it relied on a risk assessment to depart from the default position, as set out in its policy, that "*all remote network access*" would be protected by MFA. Given how dated the risk assessment is, and that no copy can now be located, it is not possible to say that BA took into consideration the risk, the state of the art, the cost, or the available technical measures when deciding what security was appropriate.
- 6.27. Moreover, BA has not identified alternative measures it put in place having reached the view that MFA was not necessary in this context.

³³ In response to paras 3.34-3.36 of BA's Second Representations, the Commissioner accepts that Citrix can be regarded as an SSL VPN, and suggests an IPSEC VPN as an alternative to – and not in addition to – the use of MFA-enabled Citrix in its role as an SSL VPN.

At paragraph 6.17 above, the Commissioner has identified alternative appropriate measures that BA could have adopted if the view was properly taken that MFA was not required, which may have justified a departure from its policy position. With respect to whitelisting:

- a. BA's First Representations³⁴ suggested that whitelisting of IP addresses would not have been effective in preventing this step of the Attack because the requests to servers within the network were coming from other servers – which would not have been whitelisted had a whitelist been in place. However, this point only applies once an attacker has gained access to the wider BA network after breaking out of the Citrix gateway. Before then, the use of IP whitelisting would have been an effective measure preventing the Attacker from gaining initial access to the Citrix Gateway. BA could have had whitelisting in place that would have ensured only certain individuals, or organisations, could access it.
 - b. In its Second Representations, BA argued that it was untenable to suggest that whitelisting was an alternative in practice due to the global spread of its users.³⁵ However: (i) there is no evidence that BA considered what alternative measures could be put in place as an alternative to MFA, which was the solution identified in its policy; and (ii) even if BA is correct that this solution would not have proven viable, it does not obviate the need to consider appropriate measures or explain why other appropriate measures were not in place, including in particular MFA.
- 6.28. BA has provided a copy of its Third-Party System Access Agreement in relation to Swissport³⁶, which included information on general password security. A contractor or third-party access policy is an agreement between two parties regarding access and any security considerations. While the Commissioner recognises that setting security standards for suppliers is commendable, the Commissioner does not consider reliance on such agreements alone to be an effective measure in ensuring that Swissport user credentials, and the access they provided to BA's systems, were appropriately

³⁴ Para 2.54.

³⁵ BA's Second Representations, para 3.37.

³⁶ Annex 9a Swissport Trinidad and Tobago – BA Third Party Systems Access Agreement.

secured.³⁷ The GDPR requires BA to take appropriate technical measures to ensure that its systems are appropriately secured. BA, through its Network Access Control Policy, appears to accept this, but failed to implement MFA as required by its own policies, or apply appropriate alternative measures.

- 6.29. For the reasons given above, BA should have ensured that MFA was in use in accordance with its policy for securing access to its network or, having carried out an appropriate risk assessment, put in place appropriate alternatives. MFA and the alternative measures identified above are readily available and mature solutions (i.e. solutions that have been known about in the industry for a long period of time, prior to the Attack), and which could have been implemented by BA without excessive cost.

Step 2: Breaking out of Citrix

- 6.30. As set out above, in its First Representations BA explained that, based on information it had obtained since receiving the NOI, it believes that the Attacker was able to break out of the Citrix environment by [REDACTED].³⁸
- 6.31. It is incumbent on BA to identify the risks associated with remote access, and to ensure that those risks are mitigated appropriately. The CAG allows remote access to internal BA applications, its infrastructure and networks. It is important that such access is configured appropriately and tested in order to mitigate against or prevent security risks, including preventing unauthorised or unprivileged users from 'breaking out' from the CAG.
- 6.32. There is guidance freely available, including from Citrix,³⁹ which identifies breakout from Citrix as a known security issue and lists effective measures to mitigate this risk.

³⁷ This agreement also referred to the DPA 1998, and had not been updated to take account of the GDPR coming into force. In response to paras 3.41-3.42 of BA's Second Representations, it should be made clear that the Commissioner does not seek to comment on the appropriateness of BA's arrangements with Swissport themselves.

³⁸ BA's First Representations, paras 2.35-2.38.

³⁹ <https://www.citrix.com/blogs/2019/04/29/citrix-tips-top-10-findings-from-citrix-environment-security-assessments/>, see para 8. See also earlier guidance published by Citrix and Mandiant in 2016, entitled "System Hardening Guidance for XenApp and XenDesktop" which states at page 2 "*Mandiant continues to observe that one of the commonly overlooked visualization security issues is environment or application jailbreaking.*"

- 6.33. In this respect, BA did not approach its obligations under Articles 5(1)(f) and 32 GDPR correctly. It did not have any up-to-date risk assessment of the CAG, or of the applications (such as [REDACTED] [REDACTED]) that were accessed through the gateway, to ensure that access to these applications was secure and could not be used to 'breakout' from the CAG.
- 6.34. As described above, [REDACTED] [REDACTED]. However, the risks of attackers using [REDACTED] to compromise systems is well-documented (and was well-documented long before the Attack).■
- 6.35. In the light of these well-established risks, appropriate security measures would have ensured that non-administrator accounts (such as the account used by the Attacker) did not have access to [REDACTED] or other software not required by such account-holders. For example, in a Joint White Paper from Citrix and Mandiant entitled "*System Hardening Guidance for XenApp and XenDesktop*" (2016)⁴¹, a number of recommendations are set out, including:

"Remove all undesired Windows and Citrix functionality – even if there appears to be no direct security threat, it is important to minimize the attack surface by removing unnecessary functionality. This includes removing:

- *All shortcuts and help keys*
- *Access to all unused ICA channels*
- *Unused Windows functionality such as pre-installed applications*
- *Access to printers or devices that are not absolutely required*
- *Especially since this often to file system access via "Print to File"*

⁴⁰ [REDACTED]

⁴¹ https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf

- Drivers that provide access to devices and services not required...”⁴²

6.36. More specifically, the white paper refers to

6.37. In addition, the Commissioner's guidance *A practical guide to IT security: Ideal for the small business* (2016), states: "each user should use an account that has permissions appropriate to the job they are carrying out at the time".⁴³ Although this guidance is aimed at small businesses, it applies *a fortiori* to large data controllers.

6.38. Similarly, the Commissioner's guidance in respect of *Security outcomes*, which applies to all controllers and processors, explains that it is necessary to:

... document and manage access to personal data and systems that process this data. Access rights granted to specific users must be understood, limited to those users who reasonably need such access to perform their function and removed when no longer needed. You should undertake activities to check or validate that the technical system permissions are consistent with your documented user access rights.⁴⁴ [Emphasis added]

6.39. That guidance document also explains that a typical example of a measure that can be taken to mitigate the risk of a cyberattack is:

⁴² https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/system-hardening-for-xenapp-and-xendesktop.pdf, page 4.

⁴³ ICO Guidance: *"A practical guide to IT security: ideal for the small business"* (2016) page 6.

⁴⁴ <https://ico.org.uk/for-organisations/security-outcomes/>

"minimising the opportunity for attack by configuring technology appropriately, minimising available services and controlling connectivity."

- 6.40. With respect to Step 2 of the Attack, there are a number of appropriate measures that BA could have taken, which would have mitigated the risk of the Attacker (or any other attacker / individual) gaining access to [REDACTED]. It would have been appropriate for BA to put in place at least one of the following measures to secure its network. Each of these options would have aided in preventing this element of the Attack, in accordance with the principle of least privilege described in the guidance above)⁴⁵, which the Commissioner expects data controllers to follow.
- 6.41. First, BA could have implemented application whitelisting. Organisations can configure their networks so that only certain programs or applications can be run by individuals gaining access to the network through a specified route. A whitelisting rule could specify, for example, that access is only granted for use of the [REDACTED] application. If an attacker then gains access, and seeks to run [REDACTED] or any other unnecessary software, that tool will be blocked because it is not on the application whitelist.
- 6.42. At the relevant time, there were various technical means by which BA could implement application whitelisting within the Microsoft Operating System, in accordance with the principle of least privilege, and which would have prevented or mitigated the risk of an attack of this kind.⁴⁶ These tools could also be used to alert administrators to attempts by third parties to access tools they do not have permission to use.
- 6.43. Second, BA could have implemented "BlackLists", which are the inverse of a whitelist and work by blocking certain applications rather than permitting them. A rule could have been put in place to

⁴⁵ See also page 3 of the ENISA Guidance entitled "*Indispensable baseline security requirements for the procurement of secure ICT products and services*" (December 2016) which describes the principle of least privilege "... whereby administrative rights are only used when absolutely necessary..." as an "indispensable baseline security requirement".

⁴⁶ There are freely available resources that come with Microsoft Server Tech, such as Software Restrictions Policies and App Locker; BA could also have purchased standalone whitelist software to provide more control.

prevent the use of [REDACTED]
or any other software not required for a particular user's role.

- 6.44. Third, BA could have completed an application/server hardening process, thereby reducing the vulnerabilities on its network. This involves, *inter alia*: (a) removing access to features that are not required for the purpose for which access is permitted; and (b) removing or restricting any protocols, software, or applications which are similarly not required. Such a process can ensure that users are only granted access to what is necessary. Again, the need to implement such measures is clear from relevant guidance. For example, the Commissioner's Guidance on *Protecting personal data in online services: learning from the mistakes of others*, published in May 2014, states: "*An important principle in network security is to only run the services that are absolutely necessary. This will reduce the number of ways an attacker might compromise systems on the network. If you have services which are publicly accessible and are not being actively used, you are exposing a range of potential attack vectors unnecessarily.*"⁴⁷
- 6.45. BA has argued that the principle of least privilege was not relevant in this case because while the Attacker gained access to BA's network via a low privilege user account, the Attacker carried out most of its activities using an account with administrator privileges.⁴⁸ This argument is misconceived. The point is that the Attacker should not have been able to break out of the CAG using [REDACTED] having gained accessed using the compromised credentials. It was the absence of necessary server hardening that allowed the Attacker to ultimately gain access to privileged credentials.
- 6.46. BA has also argued that third-party suppliers accessing [REDACTED] via Citrix will not be using a BA device, and so device hardening is not a relevant consideration in this case. However, application / server hardening are relevant measures that could have been considered. Rather than [REDACTED] as an application, it is the

⁴⁷ Para 44, <https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf>

⁴⁸ BA's Second Representations, para 3.43.

environment within which [REDACTED] was accessed, that called for a more rigorous hardening process.

- 6.47. As part of such application and server hardening BA might also have been expected to generate server documentation. This is a procedural / organisational measure that could have been put in place to aid in risk assessments and implementation of whitelists or other measures. Such documentation may include a list of software, applications and protocols required for an application to work. Such a process can help to indicate, for example, that for [REDACTED]
[REDACTED]. This, in turn, aids procedurally and organisationally with the implementation of appropriate security measures such as MFA, VPNs or software whitelisting. It also aids in risk assessment, as organisations can see clearly which pieces of software are available for execution on which systems. Unnecessary applications and/or protocols can be disabled or removed, and the list of applications that are required can be kept under closer review by identifying, for example, whether they are outdated (which can then be addressed). BA has not suggested that any server documentation was in place as part of a process of application and device hardening.
- 6.48. BA has argued that the Attacker in this case made conscious efforts to avoid detection, for example by [REDACTED]
[REDACTED].⁴⁹ However, [REDACTED] is a relatively simple step and this method of avoiding detection would not have been successful if the principle of least privilege, or any of the preventative measures identified above, had been in place. For example, had the Attacker been unable to bring any unauthorised files or programs into the environment, so that the only authorised pieces of software were those required for employee's roles (for example, by whitelisting) then [REDACTED]. Again, the measures identified above are freely available, and some are provided by Microsoft as part of the operating system used by BA.
- 6.49. BA had the opportunity to use such controls to prevent unnecessary access to certain tools. As explained above, BA now believes that Group Policies in effect at the time would have prevented the

⁴⁹ BA's First Representations, para 2.11.

Attacker [REDACTED] within the Citrix environment (which was the tool that BA's experts hypothesised may have been used in the Attack). The approach adopted by BA to these other tools is, in effect, a form of blacklist or control policy. But the same approach was not taken to [REDACTED], notwithstanding the risks that unnecessary access to [REDACTED] presented.

- 6.50. BA did disable the ability to right click on an application. This only prevented a person from right clicking it and choosing "open".⁵⁰ However, this was inadequate to prevent an attacker or other unauthorised user from opening it. The Attacker would have been able to open applications [REDACTED] by other methods, for example, by typing [REDACTED] into the file explorer tab or by selecting 'File' and 'Open' using left click.⁵¹ [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

- 6.51. Since the Attack, BA has blocked the use of [REDACTED] by adding them to the Group Policy that is believed to have prevented the use of [REDACTED] within the Citrix environment.

- 6.52. Finally, in addition to the above, there were organisational elements of BA's security procedures which allowed the failings discussed here to exist within the system for a significant period.
- 6.53. One such example is the scope of the penetration testing performed on the BA environment. BA has argued that its testing relied on [REDACTED]
[REDACTED]
[REDACTED]

⁵³

⁵⁰ BA, in its Second Representations at para 3.44, states "*It is not clear what the ICO means by 'selecting 'File' and 'Open' using left click*". For the avoidance of doubt, this means from within explorer one clicks on File > Open then browse to the PowerShell location and then double left click on Powershell.exe.

⁵¹ This is a possibility which BA itself recognises at para 2.38 of its First Representations.

⁵² BA's Second Representations, para 3.44.

⁵³ BA's First Representations, paras 2.40-2.42.

- 6.54. However, there is only evidence of [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]. Had this testing been implemented sufficiently, the ability to break out of these remote access systems into the wider network would have been identified.
- 6.55. Additionally, the Commissioner has only seen evidence of [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].
- 6.56. Had more rigorous testing been performed, or had internal penetration tests been performed (where an attacker with access to the network was simulated), many of the problems identified within this decision are likely to have been detected and appropriately addressed.

Step 3: Privileged escalation

- 6.57. Having broken out of the Citrix environment, the Attacker was able to obtain privileged access details, i.e. the details of a domain administrator account, because those details were saved in an unencrypted plain text file. This approach to storing passwords in text files is referred to as hardcoding.
- 6.58. The use of hardcoded passwords is recognised generally as being a problematic practice that increases the risk of and implications of an attack. The Open Web Application Security Project (OWASP) reported in 2016 that:⁵⁴

"The use of a hard-coded password increases the possibility of password guessing tremendously.

Consequences

⁵⁴ https://www.owasp.org/index.php/Use_of_hard-coded_password

- *If hard-coded passwords are used, it is almost certain that malicious users will gain access through the account in question.*
- **Severity:** High
- **Likelihood of exploit** Very high [Emphasis added]

The use of a hard-coded password has many negative implications - the most significant of these being a failure of authentication measures under certain circumstances.”

- 6.59. There is clear guidance in the public domain that warns about the need to apply particular protections to privileged accounts. For example, the NCSC's Guidance on *Preventing Lateral Movement*⁵⁵, published in February 2018, explains:

1. Protect credentials

All credentials on a network, especially those of administrator accounts, should be adequately protected to prevent attackers using them to gain access to devices and systems.

A common type of attack involves stealing a security token to gain access to another device or server. 'Pass the hash' is an example of this, where a stolen hash is used to authenticate the attacker. Passwords should not be stored in plain text by users or systems, and password hashes should be protected to prevent attackers easily accessing them.

...

3. Protect high privilege accounts

Local and domain administrative accounts - with access to most systems and data - are powerful tools in a network. Their use should be tightly controlled and locked down.

Administrators should use separate accounts; one for day-to-day business use (such as web browsing and emails), and a privileged administrator account that should only be used

⁵⁵ <https://www.ncsc.gov.uk/guidance/preventing-lateral-movement>

on separate admin devices. This reduces the risk of an infected device being used for admin purposes.

Administrator accounts should be prevented from browsing the web and accessing emails, and only be used when a task requires elevated permissions.

- 6.60. There were a range of appropriate measures that BA could have put in place to prevent the Attacker obtaining privileged access.

- 6.61. First, it is evident from [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

- 6.62. This same outcome could have been achieved more securely [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] The use of this readily available tool would have avoided the hardcoding of the password, and thereby prevented the Attacker from obtaining privileged access.

- 6.63. Second, BA could have adopted an approach of delegating privileges to specific admins or users (which is recommended by Microsoft⁵⁶). Instead of [REDACTED], BA could have used this delegation to limit each user's access to the tools, including administrator tools, which the individual user or users requires. This approach again reflects the "least privilege" principle, discussed above. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] using the above method

⁵⁶ See <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory>

would have been adequate, without increasing the risk by allowing all accounts domain administrator access.

- 6.64. These features / tools are freely available as part of the Microsoft Operating System used by BA. While they would not have prevented the Attack, they could have mitigated the risks associated with such an attack by permitting early detection. This early detection, if reacted to promptly, could have aided BA in removing the attacker from their network before privileged accounts were compromised and further damage was done within the BA network.
- 6.65. Generally, the risks associated with storing credentials within scripts can be mitigated with steps such as: (a) monitoring access to the script, (b) requiring the input of credentials on execution of the script, or (c) encrypting the script itself when not in use. The Commissioner accepts that due to the location and functionality of the mapping script these mitigations were not available to BA in this particular circumstance. However, this does not mean that the [REDACTED] was acceptable or appropriate, as there were other, more secure, methods of achieving the desired outcome, as outlined above.
- 6.66. Additionally, security testing of the CAG and associated applications may have identified the ability to break out of the Citrix environment. Vulnerability scanning, security testing and internal credential-based penetration testing may have identified issues associated with [REDACTED]
[REDACTED].

Step 4: [REDACTED]

- 6.67. The risks associated with [REDACTED]
[REDACTED] are well-known.
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

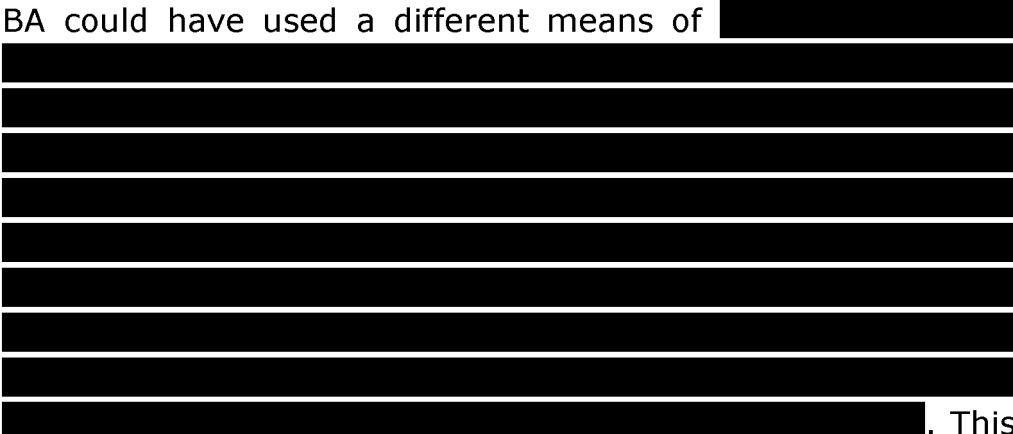
- 6.68. Systems Administrator accounts are generally disabled by default, and systems that use that account are usually legacy systems. It is

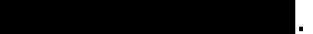
reasonable to assume that BA was aware of the security implications of the Systems Administrator account, since a decision would have to have been taken to enable that account.

- 6.69. As explained above, it is standard practice, in line with the guidance from the NCSC and the Commissioner, that systems should be configured in a way that complies with the principle of "least privilege". In practice, the Systems Administrator account should only have been enabled, when necessary, on a case-by-case basis.
- 

- 6.70. There are a number of appropriate measures that BA could have implemented to prevent or mitigate the risk of an attack of the type which occurred. In particular:

- a. BA could have implemented its own policy, which recognised the need to use different passwords for different accounts, when setting up key accounts that gave control of the whole system.

- b. BA could have used a different means of .

This would have avoided the password being saved in hardcoded form, and would have avoided the same password being set as the default .

- c. BA could have enabled .

[REDACTED]

[REDACTED]

ANSWER

The following table summarizes the results of the simulation for the two models.

Model	Number of Agents	Number of Iterations	Mean Number of Iterations to Convergence	Standard Deviation of Number of Iterations to Convergence
Model A	100	100	~10	~2
Model B	100	100	~10	~2
Model A	1000	100	~10	~2
Model B	1000	100	~10	~2
Model A	100	1000	~10	~2
Model B	100	1000	~10	~2
Model A	1000	1000	~10	~2
Model B	1000	1000	~10	~2

[REDACTED]

A large black rectangular redaction box covers the top portion of the page content, starting below the header and ending above the first section of text.

- 6.71. Alternatively, BA could have mitigated the risk presented by [REDACTED] by monitoring access to the relevant files and/or logging access to the file, which could have alerted BA to its misuse.

6.72. None of the above measures would have entailed excessive cost or technical barriers. They are all readily available measures available through the Microsoft Operating System used by BA.

6.73. The Commissioner accepts that, in some cases [REDACTED]
[REDACTED]
[REDACTED] the discovery of credentials was not useful to the Attacker.⁵⁸ However, it is still the case that the compromise of [REDACTED] was a significant step in the early stages of the Attack. For example, the [REDACTED]
[REDACTED]
[REDACTED]

57

⁵⁸ In para 3.4 of its Second Representations BA suggested that

[REDACTED] In its letter to the Commissioner of 12 October 2018, BA explained that:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- 6.74. Moreover, the Commissioner does not accept that the storage of such credentials in plain text is standard practice or an acceptable way of 'aiding functionality', as suggested by BA. The storage of passwords within scripts and configuration files prevents employees needing to enter these passwords upon the execution of the script(s), as discussed above. If this is why BA stored passwords in this way, that is not an acceptable reason to store passwords in plaintext, when considering the minimal time saving it allows, the high risk it poses, and the alternative methods (such as requiring an input of the passwords to run the script but not storing them as part of the script permanently) available to BA as an organisation. If, on the other hand, these scripts existed as part of an automatic process on the server,⁶¹ this is equally unacceptable. The Commissioner's concern is that the credentials were being stored in plain text, not why that may have been so.

Step 5: [REDACTED]

- 6.75. As described above, following failed attempts to access three servers, the Attacker obtained access [REDACTED]. Having found a hardcoded password file, the Attacker enabled the Guest Account and added it to a local admin group, thereby giving it local administrative control.

- 6.76. Microsoft's website explains:

The Guest account has been disabled by default since Windows 8 because it was determined to be a security risk.

⁶⁰ See BA's letter to the Commissioner, dated 12 October 2018.

⁶¹ See para 3.47 of BA's Second Representations, where it states that "it is possible that these scripts existed as part of an automated process on the server".

For that reason, Microsoft asked users not to use the Guest account. When you have guests, have them sign in to a local Standard user account.

- 6.77. Although the guest account was disabled on BA's system, there was no mechanism in place to detect the unauthorised enabling of that account by the Attacker. There are a number of appropriate measures that could have been put in place to detect that activity:
- Monitoring of failed attempts to log-in using the Systems Administrator account. Given that such authentication fails should not happen (as access should be carefully restricted to such accounts) the logging of failures to gain access should enable the organisation to detect activity that may be of concern. Email alerts could have been put in place to bring to the organisation's attention that there had been a number of failed login attempts;⁶² and
 - Monitoring of the use of guest accounts. The addition of the guest account to the local administrator group should have been identified by monitoring of the system. Guest accounts have been flagged as high risk, even though they have limited access to the system. Local administrators have unlimited access to the relevant system. The addition of a guest account to the local administrator group should have been detected, and would have alerted BA to a problem. But no monitoring was in place (using PowerShell or any alternative tool) that detected the unauthorised activity in this case.
- 6.78. Another option would have been the implementation of a Privilege Access Management ("PAM") audit and monitoring tool to securely manage all privileged accounts across BA's infrastructure. A PAM tool would have secured the issuing and use of a privileged account only to those users or applications that needed them, and when they needed them. The use of specific privilege accounts could have been monitored and audited following their release, to confirm usage and any relevant actions taken. Where appropriate, the account can be

⁶² Microsoft information explains how and why to implement these lockout policies, e.g. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-duration>

revoked and its password changed to protect the account from misuse.⁶³

- 6.79. Additionally, user access management is an industry wide methodology, based upon the principle of least privilege. It is identified in standards such as NIST and ISO27001 as a requirement for the management of user privileges and access to system and system resources. It is delivered through several industry recognised tools and the access management process is used to provision users, for example to applications, infrastructure and databases.
- 6.80. The Commissioner accepts that comprehensive monitoring of an IT estate as large as BA's may be a relatively complex task. However, appropriate measures to both monitor and prevent high risk actions such as the unauthorised creation of administrator accounts were available to BA. BA failed to put in place these measures, which could have prevented, or at least alerted BA, to this Attack.

Step 6: [REDACTED]

- 6.81. It is well-known that [REDACTED]
[REDACTED]
[REDACTED] There are a range of measures that can detect such activity.
- 6.82. The Commissioner notes that in this step of the Attack, the focus must be on detection rather than prevention, as the earlier failures to secure passwords and accounts meant that the Attacker was already able to move freely around BA's system.
- 6.83. A key detection measure that would have been appropriate is logging. The NCSC describe logging as "*the foundation on which security monitoring and situational awareness are built*".⁶⁵ There are a number of ways in which such logging can be implemented, including using a Security Information and Event Managing System

⁶³ See (<https://www.cyberark.com/products/privileged-account-security-solution/core-privileged-account-security/>)

⁶⁴ See [REDACTED]

⁶⁵ NCSC introduction to logging for security purposes as of 08 December 2019 - <https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes>

or using manual searches of logs to identify concerning activity, focusing on critical servers. [REDACTED]

[REDACTED] is an unusual step to take in operating a system, but is a well-known method of attack. It is, therefore, a clear sign that the system may be compromised. Such action may have been detected if it had been accurately logged.

6.84. BA had in place [REDACTED]
[REDACTED]

[REDACTED]. Had it been used to assess access management logs amongst other log files such as network logs or application logs, BA would have been alerted to the creation of or use of privileged accounts or to the elevation of a guest account to an administrator account. It could also have been used to identify brute force attacks and other high-risk actions and, given adequate scope on the network, changes to the BA website code. However, BA were not generating or monitoring logs to a sufficient level to detect these high-risk actions. This is evident, for example, in [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED] ⁶⁶

Step 7: Personal data breach; XML files

- 6.85. A failure to remove administrative or debugging functions will compromise the security of a site. This is an issue identified by, for example, OWASP in its Top 10 Insecure Configuration Management issues of 2004.⁶⁷
- 6.86. There are a number of measures that BA could have implemented which would have identified the failure to remove the debugging code.

⁶⁶ See, in particular, the "Security Monitoring" Guidance published by the National Cyber Security Centre at: <https://www.ncsc.gov.uk/guidance/c1-security-monitoring>, which notes that "*an effective monitoring strategy is required so that actual or attempted security breaches are discovered... good monitoring is more than simply the collection of logs. It is also the use of appropriate tools and skilled analysis to identify indicators of compromise in a timely manner so that corrective action can be taken.*"

⁶⁷ OWASP Insecure Configuration Management as of 08 December 2019 - https://www.owasp.org/index.php/A10_2004_Insecure_Configuration_Management

- 6.87. First, an important example of such measures is the use of manual code review. A code review is a software quality assurance activity in which one or several individuals check a program manually by viewing and reading part of its source code. At least one of the reviewers must not be an author of the code. OWASP describes this as: "*probably the single-most effective technique for identifying security flaws. When used together with automated tools and manual penetration testing, code review can significantly increase the cost effectiveness of an application security verification effort.*"⁶⁸
- 6.88. BA has confirmed that some manual code reviews did take place during the movement of code from development to production. These code reviews appear to have been sufficient to ensure that the code would do what it was intended to do. However, these reviews fall short of industry standards in many areas, especially in the review of logging code required under OWASP guidance on code reviews.⁶⁹ That guidance states that a review of any logging code should be performed to identify, amongst other things, what information should not be logged, such as sensitive personal data and some forms of personally identifiable information. BA has not suggested that it was undertaking this type of review. While the reviews were appropriate to ensure that the code operated as expected, they were not adequate to ensure that additional, appropriate security measures (such as appropriate logging) were in place.
- 6.89. Second, whilst the Commissioner accepts that the Payment Card Industry Data Security Standard ("PCI DSS")⁷⁰ does not require scanning⁷¹, the Commissioner notes that BA appears to have breached ("PCI DSS") (2008) requirement 3.1, which provides: "*Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.*" Moreover, the logging of card details was in error, rather than by design, confirming the absence of any valid business need for the processing.
- 6.90. The Guidance accompanying PCI DSS requirement 3.1 provides that: "*Extended storage of cardholder data that exceeds business*

⁶⁸ https://www.owasp.org/images/d/da/OWASP_Code_Review_Guide_-_V1_1.pdf.

⁶⁹ https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf.

⁷⁰ Payment Card Industry Data Security Standard

⁷¹ BA's Second Representations, para 3.30.

need creates unnecessary risk. The only cardholder data that may be stored is the primary account number or PAN (rendered unreadable), expiry date, name, and service code. Remember, if you don't need it, don't store it!" (original emphasis). The Guidance makes it clear that CVV numbers (the majority of which were unencrypted in this case) should not have been logged by BA at all.

- 6.91. The fact that BA did not identify that the credit card logging feature remained active after its system went live in 2015, including in particular after the GDPR entered into force in May 2018, demonstrates a failure to adopt appropriate technical and organisational measures, including regular testing, assessing and evaluation of its systems, to ensure an appropriate level of protection for customer personal data and compliance with the data protection principles, including data minimisation.

Step 8: Personal data breach; payment card data [REDACTED]
[REDACTED]

- 6.92. Attacks using [REDACTED] are well-documented as risks to systems and networks.⁷² BA could have put in place measures to detect malicious action such as that which occurred during the Attack, in particular file integrity monitoring.⁷³ This type of monitoring allows the system to detect and alert an organisation to changes being made to its code. While it does not stop an attacker from changing the code, it allows the organisation to detect that changes have been made, and to establish whether they are unauthorised.
- 6.93. PCI DSS requires (requirement 10.5.5) that merchants "*deploy file integrity monitoring software to alert personnel to unauthorised modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.*"⁷⁴ PCI

⁷² See, for example, [REDACTED]
[REDACTED]

⁷³ Having considered BA's First Representations, the Commissioner no longer refers to traffic monitoring or endpoint monitoring specifically, and considers that the relevant failure by BA was the failure to put in place appropriate file integrity monitoring and events logging on the network.

⁷⁴ Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures, Version 3.2.1, May 2018

DSS notes that, without file integrity monitoring a hacker or user with malicious intent could alter file contents or steal data undetected. The requirement set out in PCI DSS para 11.5 reinforces the point: "*Deploy a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorised modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.*"

- 6.94. BA had established manual change management controls, meaning that if an employee wanted to make any changes to BA's website, code they had to go through a formal change management process to obtain approval for that change. However, BA has not identified any technical or organisational measure it had in place to detect unauthorised changes to its website code. In this instance, BA was only alerted by a third party that significant changes had been made to the website code.

Conclusion on failures under Article 5 / 32 GDPR

- 6.95. The Commissioner's view is that the personal data stored within and processed by BA's systems, including the BA website, were not being processed in a manner that ensured appropriate security of that personal data, using appropriate technical or organisational measures. BA failed to implement appropriate technical and organisational measures to protect the rights of data subjects and comply with the data protection principles.
- 6.96. This is demonstrated by the fact that, as set out above, each step of the Attack could have been prevented, or its impact mitigated, by BA implementing one or more of a range of appropriate measures that were open to it.
- 6.97. The risks created by the way in which BA configured its network ought to have been identified by BA and resolved. Although BA was not required to implement every measure identified above, the Attack exposed BA's failure to secure its systems in an appropriate manner. There was a failure to implement appropriate measures in relation to each of the steps individually outlined above and, in particular when the failures are looked at cumulatively, the

Commissioner considers that BA was in breach of Articles 5(1)(f) and 32 GDPR.

BA's wider arguments

- 6.98. In addition to the arguments referred to above, BA's Representations raised a number of more general legal and/or factual arguments. This section addresses the following submissions made by BA:
- a. **First**, that the Commissioner was wrong to apply Article 25 GDPR in the NOI.⁷⁵
 - b. **Second**, that the Commissioner erred in her factual findings in the NOI and she could not therefore sustain her finding that BA failed to put in place appropriate measures. In particular, BA contended that the Commissioner erred by applying an "*unduly high standard*" and the benefit of hindsight.⁷⁶ BA has advanced similar arguments in its Second Representations in response to the draft decision.⁷⁷
 - c. **Third**, that the Commissioner applied an unlawful approach by failing to have regard to the whole of BA's security environment.⁷⁸ BA expended substantial efforts and applied significant resources to its preparation for the GDPR, which should also be taken into account.⁷⁹
- 6.99. As part of its wider arguments, BA also made a number of representations on the Commissioner's approach to determining whether to impose a penalty, and the methodology adopted in calculating the proposed penalty in the NOI.⁸⁰ These arguments are addressed in section 7, below.
- (1) Article 25 GDPR
- 6.100. In the NOI, the Commissioner provisionally found that BA had infringed Article 25 GDPR as well as Articles 5(1)(f) and 32. BA

⁷⁵ BA's first Representations, para 3 of the Executive Summary and paras 2.55-2.60.

⁷⁶ BA's First Representations, para 2 of the Executive Summary, and Chapter 2, in particular, paras 2.3-2.192.35-2.38. See also BA's Second Representations, paras 1.3.1, 3.15-4.43.

⁷⁷ BA's Second Representations, paras 3.1-3.48.

⁷⁸ BA's First Representations, paras 2.20-2.24.

⁷⁹ BA's First Representations, Chapter 1.

⁸⁰ Specifically, see paras 5.8-5.13, 6.13-6.28, 7.14, and 9.1-9.3 of BA's First Representations.

argued that the Commissioner had misapplied Article 25 GDPR because it was not in force at the time BA designed the relevant data processing systems and/or it should not be relied upon because it is merely duplicative in this context of the obligations applicable under Article 32 GDPR.

- 6.101. The Commissioner does not agree with BA's interpretation of Article 25 GDPR, which applies "*at the time of the processing itself*" as well as at the point at which the system is designed. The obligation applies on a continuing basis. However, the Commissioner has decided only to make findings of infringement in respect of Articles 5(1)(f) and 32 GDPR. This reflects the Commissioner's central conclusion that BA failed, as a data controller, to apply appropriate security measures meeting, in particular, the basic principles for processing applicable under Article 5 GDPR.

(2) The correct approach / standard

- 6.102. The Commissioner has considered BA's Representations on her provisional finding that BA breached Articles 5(1)(f) and 32 GDPR and her draft decision to that effect. In particular, BA submitted in both the First and Second Representations that: (a) factual findings were inaccurate; and/or (b) the Commissioner cannot maintain the conclusion that BA failed to take the available appropriate measures to remove or mitigate the risk of an attack of the kind which occurred in this case because she has applied the incorrect standard or approach.⁸¹

- 6.103. The Commissioner has clarified certain factual findings that were included in the NOI and/or in the draft decision in the light of: (a) new or additional information submitted by BA, in particular BA's new account of the likely route of the attack (via [REDACTED] [REDACTED]); and/or (b) the submissions or information provided by BA.

- 6.104. The Commissioner has summarised above her position on the relevant standard, in response to the suggestion by BA that an incorrect or appropriate standard had been applied. For the reasons

⁸¹ BA's First Representations, para 2 of the Executive Summary, and Chapter 2, in particular, paras 2.35-2.38. See also BA's Second Representations, paras 3.14-3.43.

given above, the Commissioner's view is that BA failed to put in place appropriate security arrangements as required by the GDPR.

- 6.105. As described above, there were a number of appropriate measure(s) available to BA that an organisation of its scale would be expected to take to secure its data operations. In the light of the range of measures identified above that were available to BA, and the nature of BA's processing operations, the Commissioner does not accept BA's argument that she has imposed an unduly high standard under Articles 5(1)(f) and/or 32 GDPR.⁸²
- 6.106. The Commissioner also does not accept BA's suggestion that the airline industry should not be subjected to the same security standards as other industries.⁸³ The focus should be on whether a particular data controller has taken appropriate steps by reference to the data it is processing. BA failed to take such steps. For the avoidance of doubt, this does not mean, contrary to BA's submission,⁸⁴ that the Commissioner is suggesting that the only relevant factor to assessing whether measures are appropriate is the nature of the data to be processed. In carrying out its assessment of whether BA put in place appropriate measures, the Commissioner has had regard to all of the factors listed in Article 32(1) GDPR.
- 6.107. BA's arguments seek to highlight the apparent sophistication of the criminal attack on its systems.⁸⁵ However, sophisticated cyberattacks on global businesses are commonplace. The Attack in this case was not of such a degree of sophistication as to negate BA's responsibilities for securing its system and the personal data processed within it. Many of the steps taken by the Attacker were of a kind that could have been anticipated and addressed, as they were well-known means of attempting to exploit a system.
- 6.108. In addition to the above, had the principle of least privilege been applied, the sophistication of the Attacker would have been countered. If the files that contained employee credentials had been

⁸² BA's First Representations, Chapter 2.

⁸³ This paragraph responds to a specific claim made by BA in its First Representations, paras 2.3-2.6 and, contrary to the suggestion in BA's Second Representations at para 3.18, does not seek to set out a comprehensive and general approach to the applicable standards.

⁸⁴ BA's Second Representations, paras 3.17-3.22.

⁸⁵ See, in particular, paras 2.7-2.17 of BA's First Representations.

appropriately secured, and had the tools that allowed the Attacker to perform reconnaissance been unavailable on the network, the Attacker would not have been able to take advantage of the techniques which BA describes as sophisticated.

- 6.109. The Commissioner's findings do not involve applying the benefit of hindsight in an improper manner. In identifying a range of potential appropriate measures that were available to BA, the Commissioner has found that there were clear weaknesses in BA's system that could have been identified and remedied. The failure to prevent, for example, third party users with access to BA's systems via single factor authentication from being able to access [REDACTED], was inadequate. Similarly, allowing access to hardcoded administrator passwords created clear and avoidable security risks. There was also an evident failure to put in place adequate monitoring and logging arrangements. The Commissioner does not accept that her approach to assessing the appropriateness and adequacy of BA's security measures is incorrect. Consequently, she does not accept BA's contention that its approach complied with the GDPR.
- 6.110. In its Second Representations, BA emphasises what it submits is the Commissioner's failure to put herself in BA's shoes and assess the situation as BA did at the time. BA also submits that the Commissioner erred by finding that the fact that each step of the Attack could have been mitigated or prevented because: "... *it is simply not known whether the sophistication of the Attackers was such that it would have enabled them to follow alternative attack vectors had any of the actions they took been prevented or mitigated...*"⁸⁶
- 6.111. These submissions misunderstand the nature of the Commissioner's findings. The Commissioner does not find that simply because an attack took place BA was in breach of its obligations under the GDPR. Instead, the Attack which did occur exposed the fact that BA had failed to secure its systems in an appropriate manner. This is because looking at the steps of the Attack which occurred, it is clear that there were measures it would have been appropriate for BA to put in place which would have prevented them or mitigated their

⁸⁶ BA's Second Representations, paras 3.31-3.32.

impact. The fact that the Attacker may have needed to change course or use different means to attack BA's systems if further measures had been in place does not alter this conclusion.

(3) The totality of the security environment

- 6.112. The Commissioner has had regard to BA's detailed Representations on the security measures it had in place generally.⁸⁷ However, her investigation has identified numerous appropriate measures or steps that should have been taken by BA to address the identified security risks within its system. The Attack, and/or other attacks which could have occurred as a result of the deficiencies in BA's systems mean that, even looked at in the round, BA's technical and organisational data security arrangements, including risk assessment, cannot be regarded as sufficient or appropriate.
- 6.113. The Commissioner has also had regard to BA's Representations on the steps it took to prepare for the GDPR.⁸⁸ It is notable that none of those steps identified the deficiencies in BA's security which were exploited during the Attack, notwithstanding that these could have been easily addressed by BA.

7. REASONS FOR IMPOSING A PENALTY & CALCULATION OF THE APPROPRIATE AMOUNT

- 7.1. For the reasons set out above, the Commissioner's view is that BA has failed to comply with Articles 5(1)(f) and 32 GDPR. These failures fall within the scope of sections 149(2) and 155(1)(a) DPA. For the reasons explained below, the Commissioner considers it appropriate to impose a penalty in the light of the infringements she has identified.
- 7.2. In considering whether to impose a penalty, and in calculating the appropriate amount of the penalty, the Commissioner has had regard to the matters listed in Articles 83(1) and (2) GDPR and has applied the five-step approach set out in her RAP.

⁸⁷ BA's First Representations, paras 2.20-2.24.

⁸⁸ BA's First Representations, paras 1.1-1.4.

The imposition of a penalty is appropriate in this case

- 7.3. Both the RAP and Article 83 GDPR provide guidance as to the circumstances in which it is appropriate to impose an administrative fine or penalty for breaches of the obligations imposed by the GDPR.
- 7.4. Article 83(2) GDPR lists a number of factors that must be taken into account. These are each discussed in detail below in determining the appropriate level of fine, in accordance with the steps outlined in the RAP. The points made below are also relied upon in justifying the Commissioner's decision to impose a penalty, in the light of the findings set out above.
- 7.5. The RAP provides guidance⁸⁹ on when the Commissioner will deem a penalty to be appropriate. In particular, the RAP explains that a penalty is more likely to be imposed where, *inter alia*, (a) a number of individuals have been affected; (b) there has been a degree of damage or harm (which may include distress and/or embarrassment); and (c) there has been a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it).
- 7.6. As discussed in more detail below, each of those features is present in this case. Taking together the findings made above about the nature of the infringements, their likely impact, and the Commissioner's view that BA failed to comply with its GDPR obligations, the Commissioner considers it appropriate to apply an effective, dissuasive and proportionate penalty, reflecting the seriousness of the breaches which have occurred.

Calculation of the appropriate penalty

Step 1: an 'initial element' removing any financial gain from the breach⁹⁰

- 7.7. BA did not gain any financial benefit, or avoid any losses, directly or indirectly as a result of the breach. The Commissioner has not, therefore, added an initial element under Step 1.

⁸⁹ See RAP, pages 24-25.

⁹⁰ Removing any financial gain the data controller may have obtained from the infringement is consistent with ensuring that the penalty is effective, proportionate and dissuasive (Article 83(1)), and has regard to Article 83(2)(k), which refers to "*financial benefits gained, or losses avoided, directly or indirectly, from the infringement.*"

Step 2: Adding in an element to censure the breach based on its scale and severity, taking into account the considerations identified at sections 155(2)-(4) DPA

- 7.8. Sections 155(2)-(4) DPA refer to and reproduce the matters listed in Articles 83(1) and 83(2).

The nature, gravity and duration of the failure (Article 83(2)(a))

- 7.9. **Nature and gravity of the failures:** The Commissioner considers the nature of the failures to be of serious concern. BA was processing a significant amount of personal data in an insecure manner. As set out above, there were multiple measures that BA could have put in place that would have prevented, or mitigated, the Attack.
- 7.10. The failures are especially serious in circumstances where it is unclear whether or when BA itself would ever have detected the breach. BA was only alerted to the exfiltration of personal data from its website by a third-party. In the absence of that notification, the number of affected data subjects and any financial harm to them could have been even more significant. Furthermore, the extent of any harm appears to have been limited by the fact that the Attacker appears to have been financially motivated. The Attacker could have used the access for other purposes (such as targeting high-profile individuals, disrupting customer bookings, or perpetrating other forms of fraud).
- 7.11. A significant number of individuals (429,612 data subjects on BA's estimate) were affected by the breach.
- 7.12. Notwithstanding the assurances and mitigating steps taken by BA (which are taken into account below), the Commissioner remains of the view that it is likely that many of these individuals will, depending on their circumstances, have suffered anxiety and distress as a result of the disclosure of their personal information (including payment card information) to an unknown individual or individuals. The Commissioner has considered the submissions made by BA in its Representations.⁹¹ She notes the following points:

⁹¹ BA's First Representations, paras 3.11-3.14, and 3.23; BA's Second Representations, paras 4.3 *et seq.*

- a. It is not correct that the payment card details are the only data which could arguably have *any* degree of sensitivity. Attackers may exploit combinations of names, usernames and passwords to exploit data subjects.
- b. BA's assertions as to the most likely reaction of data subjects to learning that their payment card data or other personal information has been affected do not reflect the Commissioner's experience. It is not, in the Commissioner's experience, "*inherently unlikely*"⁹² that consumers will be distressed by learning their payment card data or other personal information has been compromised. Moreover, the fact that consumers can learn how their data may be protected by third parties, such as their credit card issuer, does not remove the likelihood that they suffer distress in the interim while they establish the risks they face and how they might take steps to mitigate these risks. It is unrealistic for BA to suggest that there would not have been such an "*interim*" period between becoming aware of the breach and establishing its impact upon them.⁹³ It would necessarily take time for individuals to assess the actual risk of harm they face.⁹⁴ The fact that BA committed to reimburse financial losses in communicating the breach would not prevent an individual being distressed or concerned about the potential for such loss to occur in the first place.⁹⁵ Equally, the fact that one card company indicated that its customers did not need to take action does not mean that relevant customers would have had no concern about the implications of the Attack.⁹⁶
- c. The Commissioner does not accept that payment card breaches, at least of the type involved here, are "*an entirely commonplace phenomenon*" and therefore an "*unavoidable fact of life*", as BA claims.⁹⁷ These statements trivialise what was a serious failure on BA's part. The fact that data subjects were able to book flights online does not mean they are so "*tech savvy*" that they would be unaffected by being told that BA has lost control of their personal data as a result of its security

⁹² BA's First Representations, para 3.11.

⁹³ BA's Second Representations, para 4.3(c).

⁹⁴ BA's Second Representations, para 4.3(c).

⁹⁵ BA's Second Representations, paras 4.3(c)-4.3(d).

⁹⁶ Contrary to para 4.3(e) of BA's Second Representations.

⁹⁷ BA's First Representations, para 3.11.

failings. The Commissioner does not comment on BA's assertions that "*claimant law firms will, for entirely self-serving purposes, use the word "distress" very liberally, essentially with the aim of garnering thousands of potential claimants on no-win-no-fee agreement...*"⁹⁸ The Commissioner applies that term in accordance with the legislation, when the circumstances under consideration warrant it.

- d. As set out below, over 40,000 data subjects took up BA's offer of free credit monitoring, demonstrating that they were at least sufficiently concerned about the breach to take that precautionary step.
- e. BA's suggestion that the infringements found in this case are not serious because hundreds of thousands of data subjects were affected, rather than millions of data subjects as in other breaches to which it refers, is not accepted.⁹⁹ Given the totality of the facts and circumstances set out above, the Commissioner remains of the view that the infringements in this case are significant, and affected a substantial number of data subjects. For the reasons set out further below, BA's reliance on penalties imposed under the superseded Data Protection Act 1998 ("**DPA 1998**") regime is misplaced.
- f. The Commissioner accepts the point in BA's Second Representations¹⁰⁰ that there was a category of individuals whose CVV numbers were not compromised and that it is possible that for these individuals the risk of incurring any financial damage would be reduced compared to the category of individuals whose CVV numbers were compromised. However, the risk was not removed for such individuals. By way of example, some retailers (such as Amazon) accept card payment without CVV numbers. In any event, individuals are likely to have been distressed by the fact that their personal data had been used unlawfully.

7.13. Duration: In the NOI and draft decision, the Commissioner found that the infringement in issue lasted from 25 May 2018 (when the

⁹⁸ BA's First Representations, para 3.11.

⁹⁹ BA's First Representations, para 3.23.

¹⁰⁰ BA's Second Representations, para 4.8(b).

GDPR came into force and ended on 16 November 2018. The Commissioner remains of the view that it was reasonable to treat 16 November 2018 as the appropriate end date.

- 7.14. As BA notes in its Second Representations, the Commissioner's Lead Technical Investigation Officer asked BA in his letter of 18 February 2019 to indicate the date on which: "*the final technical measure was put in place as a result of this incident, i.e. the latest date that technical vulnerabilities brought to light as a result of this attack were fixed*". BA responded confirming that the relevant date was 16 November 2018, when its endpoint monitoring tool 'Crowdstrike Falcon' was fully deployed. Given the importance of endpoint monitoring as an appropriate measure that ought to have been in place, the date of 16 November 2018 was deemed appropriate as an end date.
- 7.15. However, the Commissioner has considered BA's submissions¹⁰¹ and decided that the infringement in issue should be regarded as continuing until 5 September 2018.
- 7.16. Thus, for the purposes of deciding whether to impose a penalty, and for calculating the appropriate amount, the Commissioner proceeds on the basis that the infringements under the GDPR commenced on 25 May 2018, when the GDPR entered into force, and ended on 5 September 2018, when personal data ceased to be transferred to BAways.com. This is a significant period of time (103 days) during which unauthorised access to, and in some cases subsequent exfiltration of, personal data went undetected by BA.

The intentional or negligent character of the infringement (Article 83(2)(b))

- 7.17. The Commissioner has had regard to the guidelines provided by the Article 29 Working Party in relation to assessing the character of the infringement in issue. It explains that:

... In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause

¹⁰¹ BA's First Representations, paras 3.15-3.19; and BA's Second Representations, paras 3.10-3.11, and 4.2.

the infringement although the controller/processor breached the duty of care which is required in the law.

It is generally admitted that intentional breaches, demonstrating contempt for the provisions of the law, are more severe than unintentional ones and therefore may be more likely to warrant the application of an administrative fine. The relevant conclusions about wilfulness or negligence will be drawn on the basis of identifying objective elements of conduct gathered from the facts of the case...¹⁰²

- 7.18. The Commissioner recognises that the infringement was not an intentional or deliberate act on the part of BA.
- 7.19. The Commissioner has, however, found that BA was negligent (within the meaning of Article 83(2)(b) GDPR) in maintaining operating systems which suffered from the significant vulnerabilities and shortcomings identified in sections 3 and 6 above.
- 7.20. In making this determination, the Commissioner places some weight on the relevant context: a company of the size and profile of BA is expected to be aware that it is likely to be targeted by attackers, sophisticated or otherwise. BA must be aware that the nature of its business involves processing large volumes of personal data, including sensitive personal data. The risk of any compromise of that information may have significant consequences for BA's customers and its own business. In view of these factors, the Commissioner would expect BA to have taken appropriate steps or a combination of appropriate steps to secure the personal data of its customers; and considers that BA was negligent (within the meaning of Article 83(2)(b)) in failing to do so.
- 7.21. BA relies upon its "extensive commitment to information security" in its First and Second Representations.¹⁰³ The Commissioner accepts that BA has been able to demonstrate commitment to certain aspects of information security, however in relation to the specific shortcomings identified in this Penalty Notice which were exploited by the Attackers, BA was negligent (under Article 83(2)(b)) in failing to ensure that it had taken all appropriate measures to secure personal data.

¹⁰² Pp.11-12.

¹⁰³ BA's First Representations, para 2.22; and BA's Second Representations, para 4.8.

- 7.22. The Commissioner acknowledges that the Attack was carried out by criminal third parties. However, the Commissioner rejects the suggestion that it is the Attackers who are primarily responsible for the breaches of the GDPR identified in this Penalty Notice. The breaches identified relate to BA's failures to comply with its obligations to put in place appropriate security measures.¹⁰⁴ These failures were exposed by the Attack. This penalty decision does not proceed on the basis that the fact of an attack justifies imposing a penalty.
- 7.23. While this penalty decision only takes into account failures under the GDPR during the period between 25 May 2018 and 5 September 2018, it is clear that the deficiencies in BA's systems were present for some time. The advent of the GDPR should have prompted a careful review of BA's systems and security arrangements. This, contrary to BA's suggestion in its Second Representations,¹⁰⁵ was evidently appreciated by BA. The Commissioner has noted that BA put in place a programme to prepare its systems for the introduction of the GDPR. However, that programme failed to identify and address the deficiencies in BA's security that were highlighted by the Attack. The Commissioner does not accept BA's argument that it did not act negligently or otherwise in breach of Articles 5(1)(f) and 32 GDPR.¹⁰⁶

Any action taken by the controller or processor to mitigate the damage suffered by data subjects (Article 83(2)(c))

- 7.24. The Commissioner has carefully considered BA's submissions to the effect that Steps 1 and 5 of the RAP are duplicative, such that BA could not discern how the mitigation action it took in response to the Attack has been taken into account.¹⁰⁷
- 7.25. The Commissioner remains of the view that it makes no difference to the ultimate decision on what, if any, penalty to impose whether the action taken by the controller to mitigate the damage is taken into account here, or under Step 5. However, she has decided to consider this issue separately under Step 5 in this Penalty Notice.

¹⁰⁴ BA's First Representations, paras 3.28-3.29; and BA's Second Representations, para 4.10.

¹⁰⁵ BA's Second Representations, para 4.8.

¹⁰⁶ BA's First Representations, para 3.29.

¹⁰⁷ BA's Second Representations, paras 5.42-5.44.

***The degree of responsibility of the controller or processor
(Article 83(2)(d))***

- 7.26. As a controller, BA is responsible under the GDPR for the security of its systems and the protection of personal data stored within those systems. It is required by the GDPR to implement security measures to reduce the vulnerability of those systems, and the vulnerability of the personal data processed within those systems, to attack. Although the initial access was gained to BA's systems through the Citrix remote access port, which was used to permit third party access to [REDACTED], it is clear that there were numerous deficiencies in BA's security measures and network which the Attack exposed.
- 7.27. The Attacker was able to exploit the deficiencies in BA's security, ultimately gaining access to personal data that should not have been accessible using the third-party remote access system. The significant inadequacies or deficiencies which the Commissioner has identified relate to the way in which BA operated its network. They were not caused by inadequacies in third-party systems or a problem with applications such as Citrix.
- 7.28. The Commissioner therefore considers that BA is wholly responsible for the breaches of Articles 5(1)(f) and 32 GDPR described above.
- 7.29. Contrary to BA's Representations, the Commissioner does not treat BA as exclusively responsible for the Attack.¹⁰⁸ Nor has she dismissed the role of the Attacker as being irrelevant.¹⁰⁹ The Commissioner appreciates that the Attacker engaged in criminal activity. She is also conscious that the Attacker gained access as a result of compromised access granted to a Swissport employee. BA did not intend anyone at Swissport to have access to the personal data processed by BA. These points do not, however, alter BA's obligations to have in place appropriate security measures. In fact, it is the possibility of such attacks by third parties that necessitate compliance with the obligations imposed by Articles 5(1)(f) and 32 GDPR. While BA submitted in its Representations that the access granted to Swissport was to a "*carefully curated set of BA applications*",¹¹⁰ that does not appear to reflect what happened in

¹⁰⁸ BA's First Representations, paras 3.39-3.45.

¹⁰⁹ BA's Second Representations, paras 4.10-4.11.

¹¹⁰ BA's First Representations, para 3.41.

practice. As described above, once onto the BA system the Attacker was able to [REDACTED] and thereafter move through BA's network, because of inadequacies in BA's security measures. It is these inadequacies for which BA is accountable.

Any relevant previous infringements (Article 83(2)(e)) or any previous failure to comply with any enforcement or penalty notices (Article 83(2)(i))

- 7.30. BA has no relevant previous infringements or failures to comply with past notices.

The degree of cooperation with the Commissioner (Article 83(2)(f))

- 7.31. The Commissioner considers that BA has cooperated fully with her investigation and has taken that into account.

Categories of personal data affected (Article 83(2)(g))

- 7.32. In the initial stages of the Attack, the data categories affected were: (a) username and passwords of contractors and employees; and (b) username and passwords of members of the Executive club. Once the malicious script was added, the categories affected were: (a) customer names and addresses; (b) unencrypted payment card data including card numbers; and (c) CVV numbers and expiry dates. The Commissioner considers the loss of control by BA of personal data such as names, addresses and unencrypted payment card data to be particularly serious, allowing as they do the opportunity for identity theft.
- 7.33. As noted above, while no "special category data" was affected, this does not mean that the data was not sensitive. CVV numbers were taken for 77,000 of the 185,000 customers who had their payment card data compromised. This meant that 77,000 customers had sensitive financial data taken, which put them at a heightened risk. The Commissioner does not agree with BA's submission that she has "*severely overstated*" the sensitivity of the data affected by the Attack or that she is treating the compromise of this sensitive data as "*commensurate with a breach of special category data*".¹¹¹

¹¹¹ See BA's First Representations, para 3.46 and BA's Second Representations, paras 4.4-4.6.

- 7.34. The Commissioner relies upon the ENISA Guidance entitled "A methodology of the assessment of the severity of personal data breaches"¹¹², which provides a scoring method to assess the severity of a personal data breach. Whilst financial data is given a score of 3 (out of a maximum of 4), the presence of an aggravating factor can elevate financial data to a score of 4. Aggravating factors identified in the ENISA Guidance, and which were present in this case, include where full financial information is disclosed and where there is a high volume of data disclosed. Therefore, the Commissioner is entitled to regard the disclosure of financial data in this case as a cause for significant concern.

Manner in which the infringement became known to the Commissioner (Article 83(2)(h))

- 7.35. BA acted promptly in notifying the Commissioner of the Attack and thereby complied with its obligations in this respect.

Conclusion at Step 2

- 7.36. Taking into account: (a) the matters set out in Sections 2-4 and 6 above; (b) the matters referred to in this section; and (c) the need to apply an effective, proportionate and dissuasive fine in the context of a controller of BA's scale and turnover, the Commissioner has determined that, in principle, a penalty of £30m would be appropriate, before adjustment in accordance with Steps 3-5 below and the application of the Commissioner's Covid-19 policy. This amount is considered appropriate to reflect the seriousness of the breach and takes into account the need for the penalty to be effective, proportionate and dissuasive.

Step 3: Adding in an element to reflect any aggravating factors (Article 83(2)(k))

- 7.37. The amount of the penalty, as identified at Step 2, may be increased where there are 'other' aggravating factors.¹¹³ In this case, the Commissioner does not consider there to be any other relevant aggravating factors. The Commissioner has not, therefore, adjusted the penalty level determined at Step 2.

¹¹² Dated 20 December 2013.

¹¹³ In accordance with article 83(2)(k) GDPR and section 155(3)(k) DPA and page 11 of the RAP.

Step 4: Adding in an amount for deterrent effect to others

- 7.38. The Commissioner is under an obligation to impose a penalty which is "*dissuasive*". The need for the penalty to be dissuasive in relation to BA itself is addressed by the analysis at Step 2. Having regard to the amount of the penalty identified under Step 2, the Commissioner does not consider it necessary to increase the penalty further under Step 4 to dissuade others.¹¹⁴
- 7.39. The Commissioner is not aware of widespread issues of poor practice that may be particularly deterred by the imposition of a higher penalty. Given BA's size and the scale of its operations, and the fact that the Commissioner has decided to impose a penalty that already takes those factors into account as part of the need to ensure that any penalty is proportionate, effective and dissuasive and to reflect the seriousness of the breach, the Commissioner considers that no adjustment is necessary under Step 4.

Step 5: Reducing the amount (save that in the initial element) to reflect any mitigating factors, including ability to pay (financial hardship) (Articles 83(2)(c) (f) and (k))

- 7.40. As explained above, in principle, other relevant mitigating factors could be taken into account under Step 2 or Step 5 of the RAP. Previously the Commissioner considered such matters in the round under Step 2 of the RAP, taking into account the factors in Article 83 GDPR and section 155(3)DPA 2018. However, in light of BA's representations, for the purposes of this Penalty Notice the Commissioner has considered relevant mitigating factors under Step 5.
- 7.41. Following the guidance set out at page 11 of the RAP, and having considered BA's representations, the Commissioner considers it appropriate to take into account the following mitigating factors:

¹¹⁴ This makes, in particular, the points made by BA at para 6.26 of its Representations irrelevant. However, it is noted that the Commissioner does not accept that she should take into account in determining whether a fine should be increased to secure a deterrent effect that a controller may have suffered reputational damage / exposure to civil claims as a result of its infringement of the GDPR. Moreover, the Commissioner does not accept that as a matter of general principle concerns about deterrent effect should be limited to deliberate breaches. It is also important to deter data controllers from acting negligently.

- a. BA took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures;
 - b. BA promptly informed the affected data subjects, other law enforcement and regulatory agencies, and the Commissioner, and fully cooperated with the Commissioner's enquiries thereafter;
 - c. Widespread reporting in the media of the Attack is likely to have increased the awareness of other data controllers of the risks posed by cyber attacks and of the need to ensure that they take all appropriate measures to secure personal data;
 - d. The Attack and subsequent regulatory action has adversely affected BA's brand and reputation, which will have had some dissuasive effect on BA and other data controllers.
- 7.42. The Commissioner has taken into account the fact that, upon being alerted to the Attack, BA acted promptly to mitigate the potential risk of damage suffered by the data subjects, including by notifying banks and payment schemes, the data subjects, and the Commissioner.¹¹⁵ In particular, the Commissioner has considered the information provided by BA about the action it took in paras 3.30-3.38 of its Representations. These included, *inter alia*, issuing a press release to 5,000 journalists and commentators, and being active on television, social media and in the press about the Attack.
- 7.43. It is also noted that BA notified the FCA, and that BA informed and co-operated with the following other regulatory and governmental bodies in the aftermath of the Attack: the UK Police, the Civil Aviation Authority, HMRC, Department of Transport, the National Crime Agency, and the National Cyber Security Centre. BA also notified other data protection regulators outside the EEA, and 21 State Attorneys General in the USA.¹¹⁶
- 7.44. The Commissioner has also taken into account the fact that BA offered to reimburse all customers who had suffered financial losses as a direct result of the theft of their card details. The offer was

¹¹⁵ Referred to, in particular, in para 3.35 of BA's First Representations.

¹¹⁶ BA's First Representations, para 3.47(c).

made on 7 September 2018 and is maintained on BA's website. BA also made free credit monitoring available.¹¹⁷

- 7.45. The Commissioner acknowledges that the steps above will have gone some way to reassuring BA's customers, and therefore may have reduced or mitigated any likely distress that may otherwise have been caused by the breach. The Commissioner does not accept, however, BA's suggestion that the action taken to mitigate the impact of the Attack would have immediately addressed all concerns on the part of data subjects about their data being in the hands of criminals and/or otherwise outside of BA's control.¹¹⁸ It is not the Commissioner's role to investigate and establish the extent of any damage that may have been caused to any particular data subject.
- 7.46. The Commissioner notes that BA has also implemented a number of remedial technical measures so as to reduce the risk of a similar Attack in future, and has indicated that expenditure on IT security will not be reduced as a result of the impact of Covid-19. The remedial measures include, in particular:
 - a. [REDACTED]
 - b. [REDACTED]
 - c. [REDACTED]
 - d. [REDACTED]
- 7.47. Having regard to the mitigating factors set out above, it is appropriate to reduce the proposed £30m penalty by 20%, i.e. to £24m.

¹¹⁷ Referred to at paras 3.34 and 3.36 of BA's First Representations.

¹¹⁸ Contrary to paras 3.37-3.38 of BA's First Representations.

¹¹⁹ BA's First Representations, paras 3.47-3.48.

- 7.48. As a result of the Covid-19 pandemic, BA has argued that any penalty should be significantly reduced, or not imposed at all because of the financial hardship it would cause.
- 7.49. The Commissioner has carefully considered BA's Third Representations and oral representations, and the evidence that BA has provided. Although the Covid-19 pandemic has had a significant short to medium term impact on BA's revenues and its immediate financial position, the Commissioner considers that the overall financial position of BA and its parent company IAG is such that the imposition of a penalty in the range being considered will not cause financial hardship.
- 7.50. The Commissioner has published guidance entitled "*The ICO's regulatory approach during the Coronavirus public health emergency*".¹²⁰ That guidance indicates that "*As set out in the Regulatory Action Policy, before issuing fines we take into account the economic impact and affordability. In current circumstances, this is likely to mean the level of fines reduces.*" While the proposed penalty will not cause financial hardship for BA, the Commissioner considers it appropriate to reduce the penalty that would otherwise have been imposed, in light of the current public health emergency and associated economic consequences. This is addressed further below, separately from Step 5.
- 7.51. The Commissioner has carefully considered BA's submissions that there are other additional mitigating factors that should be taken into account in this case.¹²¹ However, none of the points raised justify a further reduction of the appropriate penalty beyond the discounts set out above. In particular:
- a. The Commissioner has recognised that the Attack involved persistent criminal activity. But this does not alter the fact that the security of BA's network was inadequate in a number of respects, and that those failings could and should have been addressed on a prospective basis through the implementation of appropriate measures. It is BA's breaches of Articles 5(1)(f)

¹²⁰ Version 2.1, 13 July 2020.

¹²¹ BA's First Representations, para 3.47.

and 32 GDPR that are being penalised, not the actions of third parties.

- b. The Commissioner does not accept BA's assertion that no harm or damage was caused by the failings identified in this decision. It is not the Commissioner's role to investigate and establish the extent of any damage that may have been caused to any particular data subject. To the extent that BA relies on the steps it took to mitigate the impact of the Attack on data subjects, those have been taken into account.
 - c. To the extent that BA relies on other factors such as the steps it took to publicise the attack, inform relevant authorities, and the steps it has now taken to mitigate the threat of a repeat attack, those have all been taken into account in calculating the penalty and any discount.
 - d. The Commissioner does not consider it appropriate to reduce the penalty by reference to the costs to BA of taking measures to rectify or mitigate the impact of its infringement, including the cost to BA of appointing external forensic consultants or legal advisers.¹²² The fact that BA may have suffered financial losses as a result of the Attack, such as the cost of providing credit monitoring for customers or appointing external advisers, is not directly relevant to the amount of any penalty. The fact that mitigating measures were taken, in accordance with BA's obligations as a controller, has already been taken into account in calculating the overall level of penalty including any discount, and in considering whether a penalty is proportionate.
 - e. BA's preparations for the introduction of the GDPR are noted.¹²³ However, these do not undermine the Commissioner's conclusions on BA's failure to implement appropriate security measures.
- 7.52. Accordingly, having carefully considered the mitigating factors raised by BA, which are relevant to the assessment of the appropriate level of any penalty, the penalty payable by BA would

¹²² See BA's First Representations, para 3.49.

¹²³ As relied upon at para 3.50 of BA's First Representations.

be £24 million, subject to the application of the Covid-19 policy as set out below.

Application of the Covid-19 Policy

- 7.53. As described above, having regard to the impact of the Covid-19 pandemic (on BA and more generally), and consistently with the Commissioner's published guidance, a further reduction of £4m is appropriate and proportionate. The final penalty payable by BA will therefore be £20 million.

Application of the fining tier(s) (Articles 84(4) and (f) GDPR)

- 7.54. The infringement of Article 5(1)(f) GDPR falls within Article 83(5)(a) GDPR, whereas Article 32 falls within Article 83(4)(a). The appropriate tier is therefore that imposed by Article 83(a) as this is the gravest breach in issue in this case.
- 7.55. In any event, for the year ended 31 December 2017 BA has confirmed that its worldwide annual turnover was £12,226,000,000 (£12.26bn). The penalty the Commissioner has decided to impose on BA is the sum of £20 million. This is considerably less than 4%, indeed considerably less than 1%, of BA's total worldwide annual turnover, and accordingly well within the cap imposed by Article 83(5) GDPR.

BA's other representations on the decision to impose a penalty and the appropriate amount Penalty amount

- 7.56. BA submitted detailed representations in response to: (a) the Commissioner's decision to impose a penalty at all; and (b) the proposed penalty amount, as indicated in the NOI and the draft decision. The Commissioner has carefully considered those representations and, to the extent they have not already been addressed above, responds to them below.
- 7.57. In summary, BA submitted as follows:
 - a. **First**, the Commissioner misapplied Article 83(2) in deciding to impose a fine and in determining the appropriate level of penalty. A proper application of that Article should result in no

fine being imposed or, in the alternative, should result in only a low penalty.¹²⁴

- b. **Second**, the Commissioner: (i) unlawfully applied an unpublished internal document, entitled "*Draft Internal Procedure for Setting and Issuing Monetary Penalties*", in setting the proposed penalty on BA included in the NOI;¹²⁵ and (ii) calculated the revised penalty in the draft decision in a manner which was tainted by the original proposed penalty in the NOI;¹²⁶
- c. **Third**, a turnover-based approach, as adopted by the Commissioner in calculating the proposed penalty on BA included in the Notice, has no statutory basis, and is a fundamentally flawed way of achieving penalties which are effective and proportionate. The Commissioner is wrong to treat turnover as the "*core quantification metric*";¹²⁷
- d. **Fourth**, the Commissioner has applied the wrong fining Tier under Article 83 GDPR in calculating the proposed fine;¹²⁸
- e. **Fifth**, the Commissioner has acted contrary to the RAP because a proper application of that policy and/or compliance with its 'spirit' would not have resulted in a fine being issued at all, or, alternatively, would have resulted in a much lower fine.¹²⁹ In particular, BA contends that the breach in this case:
 - i. cannot be considered to be a "*most severe breach*", necessitating the imposition of a penalty, because its actions were not wilful or deliberate, the incident did not involve repeat breaches, harm to individuals, no special

¹²⁴ BA's First Representations, Chapter 2; and BA's Second Representations, paras 1.3.2, and 4.14-4.17.

¹²⁵ BA's First Representations, para 6 of the Executive Summary, and paras 4.1-4.12; and BA's Second Representations, paras 2.2-2.8.

¹²⁶ BA's Second Representations, paras 1.1, 1.3.3, 1.4, 2.7, 5.2-5.7.

¹²⁷ BA's First Representations, para 7 of the Executive Summary, and paras 5.1-5.7; and BA's Second Representations, paras 1.3.3, 5.8-5.15.

¹²⁸ BA's First Representations, para 8 of the Executive Summary, and paras 5.8-5.13; and BA's Second Representations, paras 1.3.3, 5.16-5.21.

¹²⁹ BA's First Representations, paras 9-10 of the Executive Summary, and paras 6.1-6.12, with specific representations on the application of the five-step procedure at paras 6.13-6.28 of BA's Representations. See also BA's Second Representations, paras 5.22-5.24.

- category data was affected, and BA did not make financial gains as a result of the breach;¹³⁰ and
- ii. applying the guidance in the RAP, the criteria justifying the imposition of a higher or very significant penalty do not arise in this case;¹³¹
 - f. **Sixth**, the Commissioner's penalty regime lacks legal certainty or any "*rational basis*".¹³² As a result, the Commissioner should continue to take the approach to fining under GDPR that she took in past decisions issued under the DPA 1998.¹³³ Alternatively, she should impose a fine of a level equivalent to that imposed by other European authorities under GDPR and/or impose a fine which is consistent with other decisions she has issued under the GDPR;¹³⁴
 - g. **Seventh**, the amount of the fine is not "effective" because issuing large fines is likely to be counterproductive;¹³⁵
 - h. **Eighth**, the Commissioner has failed to comply with BA's rights because: (i) the NOI failed to provide BA with adequate and clear reasoning such that a decision to proceed to impose a penalty would be unlawful because it would be contrary to BA's rights of defence¹³⁶; and (ii) her conduct post the issuance of the NOI undermined due process and therefore BA's right of defence;¹³⁷
 - i. **Ninth**, the Commissioner ought to have convened the Panel of Technical Advisers;¹³⁸
 - j. **Tenth**, in agreeing to the extension proposed by the Commissioner, BA was not given a genuine choice;¹³⁹

¹³⁰ BA's First Representations, paras 6.5-6.6.

¹³¹ BA's First Representations, paras 6.11-6.12.

¹³² BA's First Representations, Executive Summary, para 11, and paras 7.1-7.23; and BA's Second Representations, paras 1.2, 1.3.3, 5.1-5.4, 5.32-5.53.

¹³³ BA's First Representations, Executive Summary, paras 11-12, and paras 8.1-8.24; and BA's Second Representations, paras 5.54-5.60.

¹³⁴ BA's First Representations, paras 8.16-8.24; and BA's Second Representations, para 1.3.3.

¹³⁵ BA's First Representations, paras 10.1-10.5.

¹³⁶ BA's First Representations, Executive Summary paras 13-14, and Chapter 11.

¹³⁷ BA's First Representations, Chapter 12; and BA's Second Representations, paras 1.4, 2.2, 2.9-2.30.

¹³⁸ BA's Second Representations, paras 2.13-2.16.

¹³⁹ BA's Second Representations, paras 2.2, 2.17-2.30.

- k. **Eleventh**, the Commissioner has failed to comply with its statutory obligations to: (a) act in a manner which is transparent, accountable, proportionate and consistent; and (b) take into account the desirability of promoting economic growth in ensuring its actions are proportionate.¹⁴⁰

(1) Application of Article 83(2)

- 7.58. The Commissioner has described above how the factors listed in Article 83(2) apply to the facts of this case. In its First Representations, BA criticised the Commissioner's provisional findings in the NOI. It then advanced further criticisms in its Second Representations of the Commissioner's application of Article 83(2) as set out in the draft decision. Where necessary, BA's criticisms have been addressed under each step of the analysis set out above.
- 7.59. BA submits that any penalty regime engages the fundamental rights of controllers, including their fundamental right to property as provided for under Article 1 of Protocol 1 of the European Convention on Human rights, and Article 17 of the EU Charter of Fundamental Rights. The Commissioner recognises that in imposing a penalty on a controller, she must comply with relevant fundamental rights that are engaged, including under the ECHR or the EU Charter. However, it is not accepted that a penalty should only be imposed in the narrow circumstances identified by BA. Whether or not a penalty is appropriate and proportionate is a matter of judgment for the Commissioner applying, in particular, the considerations set out in Article 83 GDPR.

(2) Draft Internal Procedure

- 7.60. Prior to issuing the NOI in this case, the Commissioner had developed a Draft Internal Procedure for calculating proposed penalties, as a supplement to the RAP. Its purpose was to provide a guide, by reference to the turnover of the controller, as to the appropriate penalty. As the GDPR is a new regime, this additional tool was intended to assist the decision-makers in applying Article 83 GDPR and the RAP.

¹⁴⁰ BA's Second Representations, para 1.3.4, and Section 6.

- 7.61. BA submitted detailed representations on this issue.¹⁴¹ The Commissioner has considered those representations in deciding how to approach the calculation of the penalty to be imposed in this Penalty Notice.
- 7.62. The Commissioner remains of the view that the controller's turnover is a relevant consideration in determining the appropriate level of penalty, and this is addressed further below. However, before issuing the draft decision to BA, the Commissioner agreed that the Draft Internal Procedure should not be used in the present case. Therefore, in deciding the appropriate penalty in this case no reference has been made to the Draft Internal Procedure. The Commissioner has instead relied on Article 83 GDPR, section 155 DPA and the RAP. The approach taken to the calculation of the penalty for the purposes of this Penalty Notice is set out above.
- 7.63. Notwithstanding the fact that the Commissioner had decided no longer to rely upon the Draft Internal Procedure, BA stated in its Second Representations that the Commissioner's approach is nevertheless "tainted" by reliance upon the Draft Internal Procedure, "*given the repeated references in the DPN to the initial figure of £183 million*".¹⁴² The Commissioner does not accept this.
- 7.64. This Penalty Notice, and its earlier iteration refer (or allude) to the figure of £183 million on four occasions.¹⁴³ One reference forms part of the factual background, and the others are by reference to the fact that the proposed penalty has been reduced taking into account BA's First and Second representations. That the proposed penalty is less than the initial proposed penalty as a result of BA's Representations is simply a fact, and not an indication that the penalty calculation exercise took the initial figure as a starting point.¹⁴⁴ The process by which the Commissioner calculated the proposed penalty is set out above. The level of penalty that the Commissioner proposed to set in the past is not treated as the starting point for that consideration or factored into it.
- 7.65. BA submitted in its Second Representations that it is incumbent on the Commissioner to explain whether she has any intention of

¹⁴¹ See paras 4.1-4.12 of BA's First Representations in particular.

¹⁴² BA's Second Representations, paras 2.7, and 5.5-5.7.

¹⁴³ Draft Penalty Notice, dated 23 December 2019, paras 5.2, 7.32, 7.43, 7.68(d).

¹⁴⁴ BA's Second Representations, paras 5.2, 5.5-5.7 and 5.36-5.37.

retaining the principles behind the Draft Internal Procedure going forward.¹⁴⁵ The Commissioner has made plain in the draft decision and this Penalty Notice that turnover remains a relevant factor in assessing whether a penalty should be imposed and, if so, at what level. The Commissioner has also made plain however that the Draft Internal Procedure has not been taken into account in setting the level of penalty proposed in the draft decision or in this Penalty Notice.

- 7.66. Further, the Commissioner does not accept that the use of the Draft Internal Procedure has in any way delayed her investigation.¹⁴⁶ BA, in its First Representations in particular, provided a large volume of additional factual and technical information which the Commissioner was obliged to take into account when calculating the revised proposed penalty. That calculation exercise would have been revisited in the light of BA's extensive representations in any event. This process of consultation is part of ensuring the procedural fairness of the Commissioner's decision-making.

(3) The Use of a Turnover-Based Approach

- 7.67. BA makes two submissions at paras 5.1-5.7 of its First Representations in respect of the Commissioner having adopted a turnover-based approach.
- 7.68. The first submission is that the Commissioner should not have relied on turnover-based 'bands' defined in the Draft Internal Procedure in calculating the proposed penalty. As set out above, the Commissioner has not applied the Draft Internal Procedure in making her final decision on the appropriate penalty in this case.
- 7.69. The second submission is that the Commissioner is not entitled to use turnover-based approach at all because such an approach is inconsistent with the requirement that fines be effective, proportionate and dissuasive, and conform to the GDPR's aim of consistent and homogenous application of the rules.

¹⁴⁵ BA's Second Representations, para 2.5.

¹⁴⁶ BA's Second Representations, para 2.7.

- 7.70. In its Second Representations, BA maintains that the Commissioner continued to err in her draft decision by relying on turnover as a “*core quantification metric*”.¹⁴⁷
- 7.71. In the circumstances of this case, turnover is one of several core quantification metrics for the following reasons:
- a. A turnover-based approach is consistent with the approach taken to penalties in GDPR. The Data Protection Directive did not prescribe the level of fines that Member State authorities should impose for data breaches. The GDPR departs from that approach. In doing so, it expresses the maximum penalty in terms of a percentage of turnover. Turnover is therefore a relevant factor in determining the appropriate level of penalty to be imposed. This is also reflected in the Recitals, which make clear that the economic position of the controller is relevant even where the controller is a private person and not an undertaking: “... *Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine.*”
 - b. Further, and in any event, the Commissioner is obliged to ensure that any penalties imposed are “*effective, proportionate and dissuasive*”. Having regard to a data controller’s turnover complies with this principle by ensuring that the level of any penalty is not only proportionate but is also likely to be an effective and dissuasive deterrent for the undertaking on which it is imposed, and other equivalent controllers. It is self-evident that imposing the same penalty on an undertaking with a turnover of billions of pounds as would be imposed on a small or medium sized business would not be effective, proportionate or dissuasive. Comparable regulatory regimes that share the GDPR’s emphasis on deterrence, such as under competition law, also take turnover into account in setting penalties.
- 7.72. The Commissioner does not, therefore, accept BA’s contention that relying on turnover as a metric in calculating the appropriate penalty

¹⁴⁷ BA’s Second Representations, paras 5.8-5.15.

is “*entirely arbitrary*” because “*it bears no meaningful relationship to the wrong in issue*”¹⁴⁸, nor is it the case that such an approach will necessarily result in disproportionate fines¹⁴⁹. Turnover is a relevant metric for assessing whether any fine is proportionate and dissuasive.

- 7.73. Consequently, in calculating the penalty in this case, the Commissioner has taken into account a number of core metrics for quantification, including turnover. Turnover is one key factor to be taken into account in the round, by reference to the particular facts at issue in the case.
- 7.74. However, it is noted that BA’s primary criticism in its First Representations relates to the use of turnover bands as the starting point of the penalty calculation, and this has been addressed by the Commissioner’s decision not to rely on the Draft Internal Procedure. At para 5.4 of its First Representations and paras 5.10-5.12 of BA’s Second Representations, BA accepted that the overall financial position of an organisation may be a factor to be considered when deciding whether a fine is effective and proportionate, and/or to avoid undue hardship. BA instead emphasises that the person’s financial position should be treated only as one consideration amongst others.
- 7.75. The Commissioner agrees that a person’s financial position is a relevant factor, though not the sole factor, in determining the overall penalty. She is obliged to consider, and does consider, *inter alia*, the scale and severity of the breach and its effect on data subjects, as part of the analysis to ensure that any penalty is proportionate. However, for the reasons explained above, when considering whether a penalty is dissuasive and effective, it is also necessary for the Commissioner to consider the scale and turnover of the controller, reflecting the undertaking’s overall financial position. The appropriate penalty has to be assessed by the Commissioner in the round, applying her five-step process. She is not obliged, as BA suggests breakdown her overall assessment of the relevant penalty to distinguish between the level of fine which reflects the

¹⁴⁸ BA’s First Representations, para 5.2(a).

¹⁴⁹ BA’s First Representations, para 5.2(c).

'infringement' and the level which reflects the controller's turnover (or 'success').¹⁵⁰

- 7.76. Ultimately, the Commissioner must – before imposing a penalty – consider all relevant factors, and ensure that the penalty is effective, proportionate and dissuasive. Taking into account an undertaking's financial position as an element of that consideration is necessary and does not result in arbitrary outcomes.

(4) The Appropriate Tier

- 7.77. In response to the NOI, BA stated that the Commissioner had applied the wrong fining tier by incorrectly categorising the breaches as a "Tier 2 infringement", allowing for a maximum fine of 4% of turnover.¹⁵¹ Further representations to this effect were made in BA's Second Representations.¹⁵² BA's position was based, in summary, on the following points:

- a. There is a clear conflict in the GDPR regarding the maximum administrative fines for breaches of Articles 5(1)(f) and 32 as these impose the same core obligations but attract different maximum fines. The NOI does not distinguish between the obligations imposed by these Articles.
- b. Article 83(3) is of no assistance to the Commissioner because it only explains how the Commissioner may proceed where the same or linked processing operations infringe several "*distinct provisions*", i.e. where there is no overlap between the obligations imposed by the relevant GDPR provisions.¹⁵³
- c. The maximum fine should be 2% because:
 - i. the wording of Article 83(4) makes clear that the intention was to impose this lower maximum for breaches of Article 32. It is said that Article 83(2) makes a more explicit reference to Article 32, by referring to "*Articles... 25 to 39*", than Article 83(5)(a) does in referring to the "*basic principles of processing... pursuant to Articles 5...*" Article

¹⁵⁰ Contrary to BA's Second Representations, para 5.14.

¹⁵¹ BA's First Representations, paras 5.8-5.13.

¹⁵² BA's Second Representations, paras 5.16-5.21.

¹⁵³ BA's Second Representations, para 5.17.

- 5(1)(f) is not referred to explicitly, or as part of a continuum of sub-provisions;
- ii. Article 32 GDPR amounts to the *lex specialis* of Article 5(1)(f); and
 - iii. as Article 5(1)(f) applies only to controllers, whereas Article 32 also applies to processors, the Commissioner's approach leads to different fining regimes in respect of an identical obligation.
- 7.78. The Commissioner does not accept these submissions, for the following reasons.
- 7.79. The principle of *lex specialis* means that "*where a legal issue falls within the ambit of a provision framed in general terms, but is also specifically addressed by another provision, the specific provision overrides the more general one.*"¹⁵⁴ The Commissioner does not accept that the application of the *lex specialis* principle precludes the Commissioner from treating this case as a Tier 2 infringement.
- 7.80. Article 5(1)(f) and Article 32 are evidently distinct provisions of the GDPR, notwithstanding the degree of overlap. Article 32 applies to processors, whilst Article 5 does not. Contrary to BA's submission, there is no conflict between these provisions. They can be applied to controllers at the same time: Article 32 does not override the basic requirements laid down in Article 5(1)(f), read with Article 5(2), which establish the responsibility of the controller for demonstrating compliance with the security obligation and any breach of that principle.
- 7.81. Further, and in any event, the provisions in Article 83(4) and Article 83(5) are distinct provisions which make explicit provision for different fining tiers to apply to breaches of Articles 5 and 32 GDPR. It is clear that any infringement of Article 32 falls within the scope of Article 83(4) whilst an infringement of Article 5(1)(f) falls within the scope of Article 83(5). Article 83(4) is not more specific than Article 83(5). It is incapable of overriding it. Rather, any issue as to which maximum penalty applies is resolved by the application of

¹⁵⁴ *R (Hallam) v Secretary of State for Justice [2019] UKSC 2* at [144]. See also Case T-60/06 RENV II *Italy v Commission* (2016), at [81].

Article 83(3) which states in terms that in these circumstances “*the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.*” The legislation itself provides the mechanism for addressing circumstances in which processing engages more than one obligation.

- 7.82. The Commissioner notes that her interpretation of Articles 83(4)-(5) is supported by the Article 29 Working Party’s Guidelines on the application and setting of administrative fines for the purposes of the GDPR, which states:

Specific infringements are not given a specific price tag in the Regulation, only a cap (maximum amount). This can be indicative of a relative lower degree of gravity for a breach of obligations listed in article 83(4), compared with those set out in article 83(5). The effective, proportionate and dissuasive reaction to a breach of article 83(5) will however depend on the circumstances of the case...

*The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement. Therefore, if an infringement of article 8 and article 12 has been discovered, then the supervisory authority may be able to apply the corrective measures as set out in article 83(5) which correspond to the category of the gravest infringement, namely article 12....*¹⁵⁵

- 7.83. In any event, BA’s core objection to the use of the 4% maximum penalty appears to be its impact on the turnover-bands applied under the Draft Internal Procedure in calculating the proposed fine included in the NOI. As this approach has not been adopted in determining the final level of penalty to be imposed, the same concerns do not arise. It is noted that the final penalty imposed is well below the 2% cap, and so the application of that cap in reaching the final decision, as opposed to a 4% cap, would not have made a difference. BA is wrong to contend otherwise.¹⁵⁶ The Commissioner has considered what level of penalty is proportionate on the facts of

¹⁵⁵ Pages 9-10.

¹⁵⁶ BA’s Second Representations, paras 5.20- 5.21.

this case. The fact that this penalty is below both penalty caps merely shows that a dispute over which cap should apply would be academic.

(5) Application of the RAP

- 7.84. In response to the NOI, BA submitted that the Commissioner had acted contrary to the RAP in: (a) deciding to impose a penalty at all in this case; and (b) in setting the proposed level of fine. BA relied in this regard on the public law obligation on an authority to comply with its published policies unless there is a good reason for any departure.¹⁵⁷
- 7.85. The Commissioner has complied with her published policies in preparing the NOI and making her final decision in this case.
- 7.86. First, the Commissioner has not acted contrary to the RAP by deciding to impose a penalty on BA. At paras 6.5-6.6 of its First Representations and para 5.24(a) of its Second Representations, BA misunderstands and/or misapplies the guidance at page 25 of the RAP:
- a. A breach does not need to qualify as a "*most severe breach...*" for the Commissioner to issue a penalty notice. The guidance quoted by BA explains only that in the majority of cases the Commissioner will reserve her powers for the most serious cases. The RAP does not introduce a new criterion that a case must qualify as a "*most severe*" breach before the Commissioner will apply a penalty in accordance with Article 83 GDPR and the RAP (and the latter must be read and understood in the context of the EU law regime).
 - b. In any event, the types of the "*most severe*" breaches which the RAP explains are likely to result in a penalty notice being issued include cases of "*negligent acts*". The Commissioner has found that BA acted negligently (within the meaning of the GDPR) in this case.¹⁵⁸

¹⁵⁷ BA's First Representations, paras 6.1-6.12; and BA's Second Representations, paras 5.22-5.24.

¹⁵⁸ BA's First Representations fail to accurately reflect the totality of the Guidance provided in the RAP. While page 25 refers to the fact a penalty is more likely to be imposed where it involves "*wilful action*", the RAP also makes clear that the extent of negligence involved in a breach is relevant to deciding whether to impose a penalty and, if so, the amount;

- c. The RAP does not list the “*criteria*” which make a penalty more likely to be imposed. Page 25 of the RAP provides examples of circumstances where it is more likely for a penalty to be imposed. These are expressly described as “*examples*” and there is no suggestion that either the list is exhaustive, or that all or many of the circumstances have to be present before the Commissioner can consider the imposition of a penalty to be appropriate. Any such approach would unduly fetter the Commissioner’s regulatory discretion.
- d. In any event, the facts of this case: (i) satisfy a number of the “*criteria*” or, more accurately, fall within the examples given at para 25 of the RAP and/or (ii) fall within the relevant considerations at page 24 of the RAP. Contrary to para 6.6 of BA’s Representations, the infringements in this case:
 - i. affected a significant number of data subjects, and the fact that other breaches have also involved millions of data subjects does not detract from this point¹⁵⁹;
 - ii. are likely to have caused a degree of damage or harm; and
 - iii. involve “*a failure to apply reasonable measures (including relating to privacy by design) to mitigate any breach (or the possibility of it)*”. BA’s Representations state that this example is “*not applicable*”. For the detailed reasons given above, BA’s position is not correct.

- 7.87. Second, the Commissioner has not erred by failing to apply the “*criteria*” set out at page 27 of the RAP for applying a higher penalty.¹⁶⁰ This submission is based on a misreading and misapplication of the RAP.
- 7.88. The types of cases included at page 27 of the RAP are not a list of “*six criteria identified by the ICO as meriting a “higher” penalty*”.¹⁶¹ As page 27 states, it is a list of examples of the type of situation where, generally, the amount of penalty will be higher. This passage relists a selection of the aggravating factors referred to at page 11 of the RAP and explains – perhaps self-evidently – that where those

¹⁶⁰ BA’s First Representations, paras 6.10-6.12.

¹⁶¹ BA’s First Representations, para 6.12.

factors exist, a data controller can, generally speaking, expect the penalty to be higher than where they do not exist, in the case of otherwise similar breaches.

- 7.89. The examples provided are not to be applied as a list of criteria which must be met in any case before a penalty exceeding £1 million can be imposed, as BA appears to imply in its submissions. This section of the RAP does not refer to the concept of "*very significant*" penalties at all. This language is used only to describe the types of situations in which the Commissioner may convene an advisory panel.¹⁶² While the RAP describes "*very significant*" penalties as "*expected to be those over the threshold of 1M*", this was not intended to be - and in any event cannot objectively be read as - giving an indication to controllers of the likely penalty they may face in the event of a data breach, particularly in light of the provisions of the GDPR.
- 7.90. The GDPR was enacted in 2016 and came into force two years later. Data controllers, especially global undertakings of the size of BA, would have been fully aware of the maximum penalties permitted by GDPR. The reference to the sum of £1 million in the RAP does no more than describe the circumstances in which the Commissioner may decide to convene an advisory panel. The decision as to whether a penalty should be imposed and at what level, in order to provide an effective, proportionate, and dissuasive result has to be reached through the application of Article 83(2) GDPR and section 155 DPA. It is clear from the RAP that the Commissioner will adopt a case-specific approach, taking into account all relevant considerations. That is the approach taken in this case.
- 7.91. Third, the Commissioner has taken into account, insofar as necessary, BA's own approach to applying the RAP to this case.
- 7.92. Paras 6.13-6.28 of BA's First Representations consist of BA's own application of the five-step penalty setting process. The Commissioner has considered those representations. She notes that:

¹⁶² Page 26 of the RAP.

- a. To the extent that the Representations raise concerns about the application of the Draft Internal Procedure and/or the use of turnover bands, they have been addressed above.¹⁶³
 - b. The Commissioner has applied correctly each of the limbs of Article 83(2) in this case. For example, the fact that the breach was not intentional is not the only consideration that is relevant under Article 83(2)(b), contrary to para 6.17 of BA's Representations. Article 83 also requires consideration of whether BA's actions were negligent, within the meaning of the GDPR (which the Commissioner has found to be the case).
 - c. The distinction drawn by BA between imposing a fine for the infringement of the GDPR and not the "*personal data breach*" is not a good one.¹⁶⁴ Clearly, in establishing the nature and gravity of the infringement, including the impact on data subjects, regard must be had to the impact of the personal data breach.
 - d. The Commissioner has decided on a reduced level of penalty, having taken into account BA's Representations.
 - e. BA is wrong to rely on cases issued under the previous DPA 1998 regime to calculate the penalty applicable under the new EU regulatory framework.¹⁶⁵
 - f. Concerns about the draft of internal records of the ICO's early decision-making,¹⁶⁶ prior to the issuing of both the NOI and this decision, are no longer relevant. As has been made clear in both the NOI, and this decision, the Commissioner has not increased the penalty at Step 3 of the process as she has not found there to be any aggravating factors in this case.
- 7.93. It is noted that in Chapter 9 of its First Representations BA applies the five-step process again, but on the basis of: (a) the Commissioner being constrained by the fine levels that were imposed under DPA 1998; and (b) the levels of fines imposed by other EU regulators in the relatively few decisions made under the

¹⁶³ BA's First Representations, paras 6.13, 6.16, 6.18, 6.23, 6.28.

¹⁶⁴ See para 6.18 of BA's First Representations.

¹⁶⁵ BA's First Representations, paras 6.20, 6.23-6.25.

¹⁶⁶ BA's First Representations, paras 6.21-6.22.

GDPR to date and/or a single guidance document from another authority. For the reasons provided in detail below, the Commissioner does not accept that she is constrained to apply the RAP in this manner, which would be contrary to Article 83 GDPR. Thus, while she has considered BA's calculation of an alternative fine premised, in particular, on comparisons with fines issued under DPA 1998, BA's arguments do not alter the Commissioner's conclusions on the proper application of Article 83 GDPR and the RAP in this case, set out above.

- 7.94. In BA's Second Representations, BA sets out an alternative application of the Article 83(2) criteria, as part of its claim that the revised penalty proposed in the draft decision is wholly disproportionate. This alternative application reflects the differences in position between the Commissioner and BA on a number of issues relevant to determining whether any penalty should be imposed and, if so, at what level. In particular, BA disagrees with the Commissioner's judgment as to the seriousness of the infringement and its impact on data subjects, the negligent character of the infringement, the degree of responsibility on the part of BA, the categories of personal data affected. The Commissioner has responded to BA's case on these matters above. However most fundamentally BA entirely ignores Article 83(1) and the obligation on the Commissioner to ensure that any penalty it imposes is "*effective, proportionate and dissuasive*". Any attempt to recalculate the overall penalty, and particularly where the claim is that it is "*wholly disproportionate*" must have regard to this obligation.¹⁶⁷

(6) Legal Certainty and the approach adopted under DPA 1998

- 7.95. In its Representations in response to the NOI, BA emphasised that:
- the proposed penalty engages its fundamental property rights; and
 - as a result, the penalty regime applied under DPA must have sufficient certainty to protect against arbitrariness.
- 7.96. BA's position is that the current regime does not provide that necessary certainty. Consequently, BA states that the Commissioner

¹⁶⁷ BA's Second Representations, paras 4.14-415 and page 30.

should continue to apply penalties in a manner which is consistent with the approach she adopted under the superseded DPA 1998 regime, or with the limited decisions or guidance issued to date by the other supervisory authorities under the GDPR.¹⁶⁸

The alleged lack of legal certainty

- 7.97. As set out above, the Commissioner recognises that in imposing a penalty on a controller, she must comply with any relevant fundamental rights that are engaged, including under the ECHR or the EU Charter. The Commissioner does not accept that the penalty regime applicable under, in particular, Article 83 GDPR (and section 155 DPA) lacks sufficient certainty such that it cannot be lawfully applied in conjunction with the RAP.
- 7.98. First, in para 7.8 of its First Representations, BA attacks the DPA as failing to provide guidance beyond the requirement that it pay due regard to specified matters. However, the DPA reflects the directly applicable EU law framework for assessing penalties. The Commissioner does not agree with BA that Article 83 GDPR or section 155 DPA are so unclear that they are unlawful. Taken together, those provisions specify the circumstances in which a data protection authority has the power to impose an administrative penalty, and the matters that are relevant to that decision and the amount of any penalty.
- 7.99. BA seeks to compare section 155 DPA and section 55A DPA 1998. That comparison is inapt. The latter provision was enacted in domestic law in a context where the 1995 Data Protection Directive did not specify how national regulators should make decisions about penalties. The field has now been occupied by Article 83 GDPR. The GDPR regime, which is directly applicable law, was specifically designed to strengthen the enforcement of data protection rights across Europe.
- 7.100. Further, and in any event, section 55A of the DPA 1998, on which BA relies, gave the Commissioner a discretion as to whether to impose a penalty, where a number of factors were satisfied. These included the seriousness of the contravention, its impact on data subjects, and the degree of culpability on the part of the controller.

¹⁶⁸ BA's First Representations, paras 7.1-7.23.

These criteria are comparable, in terms of specificity, with the provisions of the DPA, which require the Commissioner to have regard to Article 83(2). The factors listed in Article 83(2) include, in substance, all of those under section 55A of the DPA 1998, as well as a number of additional factors. The Commissioner was and remains required to exercise her judgment as to, for example, the seriousness and nature of any contravention, in deciding whether to impose a penalty. Thus, even if the comparison were relevant, the Commissioner does not accept BA's attempt to distinguish the current and old regimes.

- 7.101. Second, BA contends that it is not challenging the legality of the GDPR legislative regime itself. Instead, it says that Articles 83(8)-(9) and 70(1)(k) GDPR "*directly envisage and expect*" that the high-level principles set out in the legislation will be the subject of national or supranational guidance.¹⁶⁹ In fact, Article 83(8)-(9), make no mention of the need for guidance in order for Articles 83(1)-(6) to be applied lawfully (see above). Article 70(1)(k) provides that the European Data Protection Board can on its own initiative or at the request of the Commission issue guidelines about the setting of administrative fines. However, the application of Article 83 is not made contingent upon the Board doing so, and the Board has in fact adopted the guidelines issued previously by the Article 29 Working Party. This decision (and the NOI and draft decision) are consistent with that guidance.
- 7.102. BA also relies on the fact that pursuant to section 160 DPA the Commissioner is obliged to issue guidance in respect of how she will determine the amount of penalties to be imposed. However, the Commissioner has done so. In accordance with s. 161 DPA, the RAP was laid before Parliament for approval, and was duly approved. Ultimately, BA's challenge is against the RAP, but that guidance has to be read alongside the obligations imposed on the Commissioner by Article 83 GDPR, and section 155 DPA, in respect of the correct approach to imposing fines.
- 7.103. Third, turning to the guidance issued by the Commissioner, BA criticises the RAP as being too vague to satisfy the requirements of

¹⁶⁹ BA's Second Representations, para 5.46.

legal certainty. More specifically, it is necessary to address the following points BA makes in this regard:

- a. First, that the ICO's previous guidance on penalties under the DPA 1998 was longer or more detailed. However, this is a complaint of form, not substance. If the guidance provided by the RAP, taken together with the legislative regime, satisfies any relevant requirement of legal certainty, it is not relevant whether previous guidance was longer and/or provided across more than one document.¹⁷⁰
- b. Second, BA refers to the fact that the old guidance was a separate document, and not provided as part of the RAP in place at that time. Again, this is a complaint of form and not substance.¹⁷¹
- c. Third, BA claims that it follows from the development of the Draft Internal Procedure that the RAP is deficient¹⁷² and/or that it follows from the abandonment of that Procedure that the Commissioner no longer has a methodology upon which to base its proposed penalty.¹⁷³ These points are incorrect:
 - i. The Draft Internal Procedure is no longer relied upon and, in any event, it was not developed in order to 'cure' a gap in legal certainty.¹⁷⁴ It was intended to be a helpful supplement to the RAP for internal decision-making purposes. The GDPR is a new regime. More detailed guidance may be developed over time as the UK and EU Member States gain experience in applying it. The ICO may well seek to publish further guidance in the future on penalty-setting. But the potential for further development is not equivalent to the present guidance being so unclear as to be unlawful. The RAP provides sufficient guidance as to the circumstances in which penalties, including large penalties, will be applied. The Commissioner therefore does not accept BA's argument that the RAP is "*clearly insufficient*".

¹⁷⁰ BA's First Representations, para 7.9.

¹⁷¹ BA's First Representations, paras 7.9-7.11

¹⁷² BA's First Representations, paras 7.11-7.15.

¹⁷³ BA's Second Representations, paras 5.32-5.41.

¹⁷⁴ Contrary to the submissions at paras 7.12-7.13 and 7.15. of BA's First Representations.

- ii. The Commissioner has applied the approach set out in her RAP, and considered the factors identified under Article 83 GDPR. In paras 7.1-7.55 above, the Commissioner has explained each relevant step of the calculation. The Draft Internal Procedure was consistent with this approach. The Commissioner does not therefore accept that without the Draft Internal Procedure it is impossible for her to lawfully calculate a penalty, she also does not accept that the legislation and Parliamentary-approved RAP leave any “*lacuna*”.¹⁷⁵ This argument in respect of legal certainty is addressed in more detail below.
- d. Fourth, BA claims that the penalty setting process set out in the RAP is too opaque, and thereby prevents BA’s effective scrutiny of the Commissioner’s quantification analysis. Specifically, BA claims that only a “*systematic and transparent calculation methodology in the context of the quantification exercise*” will provide sufficient legal certainty to allow the Commissioner to impose a penalty.¹⁷⁶ It is not accepted that the 5-step process set out in the RAP is opaque, or in fact that any guidance could permit a controller to calculate specifically what any fine might be. The guidance has to cover a wide range of potential situations. In any event, to assist BA, the Commissioner has dealt with the mitigating factors arising in this case under Step 5 of the analysis so that it can see the impact of these on the overall level of penalty.

7.104. The GDPR is a new regime. More detailed guidance may well be developed over time as the UK and EU Member States gain experience in applying it. As BA highlights, the Commissioner has committed to updating its guidance in the future. But the potential for further development is not equivalent to the present guidance being so unclear as to be unlawful (contrary to para 5.45 of BA’s Second Representations). The RAP provides sufficient guidance as to the circumstances in which penalties, including large penalties, will be applied.

¹⁷⁵ BA’s Second Representations, paras 5.33-5.34.

¹⁷⁶ BA’s Second Representations, paras 5.36-5.40.

- 7.105. Fourth, BA's argument appears to be that because it is possible for the RAP to be more detailed, it must follow that the RAP is insufficiently detailed to fulfil the requirements of legal certainty. The Commissioner considers that the RAP, which must be read alongside the DPA and the GDPR, provides sufficient clarity and legal certainty, as required under the ECHR and EU law. The RAP explains that Step 2 intends to "*censure*" the breach, and this requires taking into consideration its scale (including the number of data subjects affected) and the severity of the breach itself, and expressly refers to the factors set out in the DPA. Where these are not already considered by reason of Article 83(2)(a)-(j), examples of aggravating factors are set out in the RAP to assist with the interpretation of Step 3, as well as mitigating factors (Step 5).
- 7.106. Fifth, BA also criticises the five-step procedure set out in the RAP on the basis that it is confused and internally contradictory. It is claimed that if Step 2 is complied with properly, Steps 3-5 are rendered duplicative and/or redundant.¹⁷⁷ In a holistic assessment of a penalty, in accordance with Article 83(1)-(2), the five-step process could in theory be applied in a way that results in overlap. However, the Commissioner has made it clear above at which step in the process the relevant factors, as defined in Article 83 and the RAP, have been taken into account in assessing whether to impose a penalty, and in determining the amount. There is no unlawful uncertainty in the approach taken by the Commissioner. In any event, as explained above, the Commissioner has altered how she addresses the potential overlap in this final penalty notice to provide additional transparency as to her approach, in the light of BA's submissions in this regard.
- 7.107. Sixth, having submitted in its First Representations that the Commissioner's reliance upon the Draft Internal Procedure, which had provided such a quantification methodology, contravened the principle of legal certainty, BA's position in its Second Representations is that the Commissioner has erred by not relying upon a clear and certain quantification methodology as that is also a breach of legal certainty.¹⁷⁸ Yet, BA accepts that the principle of legal certainty does not require the Commissioner to publish a RAP

¹⁷⁷ BA's First Representations, para 7.14; and BA's Second Representations, paras 5.42-5.44.

¹⁷⁸ BA's Second Representations, paras 5.32-5.47.

which allows a controller such as BA to predict exactly the sum of any penalty which may be imposed.¹⁷⁹ The penalty calculation process set out in the RAP was approved by Parliament and, to some extent, reproduces the considerations under Article 83 of the GDPR which is a directly effective harmonising measure. Legal certainty does not require BA to know exactly how the different factors are weighted by the Commissioner in this case. It is sufficient that BA knows a) what those factors are, b) at what stage of the penalty calculation process those factors will be taken into account; c) the need for any penalty to be effective, proportionate and dissuasive, and d) that considering turnover is relevant to (c). The Commissioner has taken into account all of the factors referred to above, these factors were looked at in the round, giving careful consideration for the overall requirement under Article 83(1) for a penalty to be proportionate and dissuasive.

7.108. Thus, the Commissioner not accept BA's argument that the RAP is "*clearly insufficient*". Consequently, the Commissioner does not accept BA's arguments as to the requirements of legal certainty in this context, nor the contention that, taking Article 83 GDPR, the DPA, relevant EDPB guidance¹⁸⁰ and the RAP as a whole, "*it is impossible for controllers (or anyone else) to assess how the ICO will exercise its fining powers...*"¹⁸¹

7.109. The Commissioner notes that BA, at paras 7.17-7.20 of its First Representations, relies upon the penalty-setting guidance of the CMA. The Commissioner has considered penalty setting in other regulatory contexts. She recognises that each regulator must take enforcement action within the bounds of its own legal obligations, and in this case the Commissioner is bound to comply with Article 83 of the GDPR.

Application of the DPA 1998

7.110. BA's solution to the alleged lack of legal certainty in the new EU law regime, read together with the RAP, is for the Commissioner to adopt an approach to fines under Article 83 GDPR which is consistent with its previous enforcement decisions under the DPA 1998 (para

¹⁷⁹ BA's Second Representations, para 5.59.

¹⁸⁰ See Article 29 Data Protection Working Party Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, which refers to

¹⁸¹ BA's First Representations, para 7.16. See also BA's Second Representations, paras 5.35-5.45.

7.23 and Chapter 8 of BA's First Representations). What BA seeks, in effect, is for the Commissioner unilaterally to impose the previous domestic cap and approach to fines which applied in the UK prior to the EU issuing the harmonised regime under the GDPR.

7.111. Plainly it is not open to the Commissioner, as a matter of domestic or EU law, to adopt unilaterally an approach that would undermine the object and purpose of the new EU regime. The GDPR, and consequently the DPA, represent a significant departure from the regime under the DPA 1998 and the 1995 Directive. The GDPR was expressly intended to harmonise the rights of, and protections afforded to, data subjects across the EU. It differs markedly from the 1995 Directive, most obviously in that it introduces significantly higher and more effective penalties, with maximum penalties defined expressly by reference to turnover. The GDPR also imposes new obligations on controllers, including new organisational requirements such as the designation of a data protection officer and new provisions on the lawfulness of processing. The GDPR and the DPA have significantly changed the legal landscape in data protection and enforcement.

7.112. BA's First Representations at paras 7.23 and 8.1-8.11 are to the effect that the Commissioner should, in the alleged absence of legal certainty under the current regime, maintain the position under the DPA 1998. Such an approach would be inconsistent with the obligations imposed on the United Kingdom and the Commissioner by the GDPR and EU law.

7.113. The points made above are unaffected by any public statements that may have been made by the Commissioner or her staff. Those statements to which BA refers have been quoted selectively and/or taken out of their proper context by BA. BA disputes this,¹⁸² however the Commissioner maintains her position for the following reasons:

- a. BA refers to a blog post published by Elizabeth Denham on 9 August 2017.¹⁸³ Whilst it is true that the post states that the Commissioner will not "*simply scale up penalties*" issued under the DPA 1998, it also states that "*Don't get me wrong, the UK fought for increased powers when the GDPR was being drawn*

¹⁸² BA's Second Representations, paras 5.54-5.60.

¹⁸³ BA's First Representations, para 8.14(a).

up. Heavy fines for serious breaches reflect just how important personal data is in the 21st century world. We intend to use those powers proportionately and judiciously."

- b. BA refers to a speech made by James Dipple-Johnstone at the Data Protection Practitioner's Conference on 9 April 2018,¹⁸⁴ however the quotation which BA selectively cited is preceded by a summary of the approach the Commissioner intended to take, including "*we will look at each case on its own merits. We'll look at the features and context of each case. And, this is important, we will focus on area of greatest risk to people – potential or actual harm... The more serious, high impact, deliberate, wilful or repeated breaches can expect the most robust response.*"
- 7.114. In this decision, and as set out in the penalty calculation above, the Commissioner has not "simply" scaled up penalties, or added zeros to the maximum penalty applicable under the DPA 1998.¹⁸⁵ None of the statements made by the Commissioner or her office can be relied upon as creating a legitimate expectation that the Commissioner will not fully apply the provisions of the legal regime under the DPA and the GDPR. More specifically, the public statements referred to by BA at paras 8.12-8.15 of its First Representations (and contextualised above) were not intended to be – and cannot objectively be read as – assurances to any controller that the Commissioner would not use her full powers on a case by case basis, to impose effective, proportionate and dissuasive penalties in appropriate cases, which includes the possibility of large fines where appropriate.

Other decisions by the Commissioner / decisions by other European authorities

- 7.115. BA submits¹⁸⁶ that the proposed penalty is: (a) inconsistent with previous action by other EU supervisory authorities, contrary to the stated aim of the GDPR being to create a harmonised regime; and (b) inconsistent with a decision reached by the Commissioner in a different case. In particular, BA's Representations imply that the

¹⁸⁴ BA's First Representations, para 8.14(b).

¹⁸⁵ BA's Second Representations, para 5.55.

¹⁸⁶ BA's First Representations, paras 8.16-8.24. BA's Second Representations, paras 5.25-5.31.

appropriate penalty in this case should be set at a level consistent with those imposed by:

- a. the Romanian authority on UniCredit Bank SA. The company was fined of €130,000 for a breach of Article 25 GDPR due to the compromise of payment details, when its worldwide turnover for 2018 was of €18 billion;
- b. the Portuguese authority on a hospital. The hospital was fined €400,000 for the incorrect handling of patient records;
- c. the Austrian Data Protection Authority against Österreichische Post AG, which was fined €18 million;
- d. a €2.6 million fine issued by the Bulgarian Commission of Personal Data Protection to the Bulgarian Revenue Agency in relation to a cyber attack which affected over 5 million data subjects; and
- e. the Commissioner's decision regarding Doorstep Dispensaree Ltd, dated 20 December 2019.

7.116. The purpose of GDPR is to secure a harmonised regime. However, in the first instance, that harmonisation is achieved through the application of harmonised rules and standards to the particular facts of the case at issue. Any cross-border processing decision must then be subject to the Article 60 process.

7.117. The Commissioner, along with other EU supervisory authorities, must comply with her obligations under Article 83 and that means that she is required to impose a penalty which, in her own judgment, having regard to all the matters listed in Article 83, and on the facts of the individual case, is effective, proportionate, and dissuasive. In principle, 'equivalent' breaches should attach 'equivalent' penalties. But in practice, each case must turn on its own particular facts. Whilst the Commissioner has considered the limited information available about the cases to which BA has referred, she maintains that simple comparisons of the penalties imposed in different cases do not show that the Commissioner has erred in applying Article 83 GDPR, DPA and/or the RAP.

- 7.118. There is a great degree of variation in the penalties imposed by supervisory authorities even in the context of the limited fines imposed to date,¹⁸⁷ which are – in the Commissioner’s view – indicative of a decision-making process that is fact-specific. The Commissioner further considers that it would be premature and not necessarily helpful to rely heavily at this juncture on a survey of the action taken by other supervisory authorities, given the relatively few decisions that have been taken under the new regime. This is particularly the case where there is limited public information available about the reasons for the decisions taken by other authorities.
- 7.119. As to BA’s reference to the guidance published by the Netherlands SA, the Commissioner does not consider that the approach can be distinguished in principle from that of the Commissioner or that the level of penalty – had this matter been before the Netherlands SA – would necessarily have been very different. The guidance leaves open the possibility that, having regard to all of the factors set out in Article 83, the Netherlands SA would consider that in BA’s case a penalty above 1,000,000 Euros was appropriate.
- 7.120. Further, as to the comparison drawn by BA between the policy of the Netherlands authority, and the Commissioner’s former Draft Internal Procedure,¹⁸⁸ in the light of the points made above, those concerns no longer arise.
- 7.121. In any event, as the Commissioner is acting as lead authority in this case, the way to ensure that consistency is not by comparing the penalty to a selection of other penalties issued on different facts in the EU. Rather, the consistency mechanism provided for by Articles 60(4) and 63 GDPR will allow for all of the supervisory authorities concerned to cooperate with the Commissioner, make enquiries, and contribute their views in order to ensure the consistency of the ultimate penalty sum with penalties that have been (if there are any) and/or will be applied in similar situations. Contrary to BA’s Second Representations, the Commissioner does not “*simply rely*” on the

¹⁸⁷ Notably the decision of the French SA, the CNIL, to fine Google 50 million Euros. See also <https://www.enforcementtracker.com/> which suggests there is significant variation in the level of fines that have been imposed to date, ranging from a few thousand to millions of pounds.

¹⁸⁸ BA’s First Representations, para 8.22.

consistency mechanism to ensure consistency.¹⁸⁹ However, the Article 60 process is one of the factors which, as noted in Article 63, contributes to the consistent application of the GDPR and the Commissioner is entitled to rely on the process as a contributory factor.

(7) Effectiveness

- 7.122. The Commissioner does not accept BA's submission that imposing a large penalty will necessarily have a chilling effect on the self-reporting of breaches. On the contrary, given the powers of the ICO to impose a sufficiently dissuasive penalty, and the fact that failing to report a breach or otherwise cooperate with an investigation are aggravating factors when calculating the penalty sum, the Commissioner considers it unlikely that controllers will decide not to report a major breach as a result of the level of the penalty imposed on BA. This is particularly so in circumstances where BA has been given a penalty reduced from the level proposed in the NOI, and that expressly takes into account early notification and cooperation, which is likely to encourage such conduct by other controllers in the future.
- 7.123. The Commissioner notes that the revised penalty of £20m is considerably lower than the original proposed penalty, having taken into account BA's detailed Representations.

(8) Rights of the Defence

- 7.124. BA advances two criticisms of the Commissioner's procedure in respect of the NOI, on the basis that she has failed to comply with the rights of the defence.
- 7.125. First, it is suggested that the NOI does not comply with the public law requirement that it must be properly and fully reasoned, and it is also too brief (as is the Commissioner's record of her internal decision-making process).¹⁹⁰ Second, it contended in the First Representations that the Commissioner's conduct between the issuing of the NOI undermined due process and BA's right to a defence.¹⁹¹ Third, in its Second Representations it made similar

¹⁸⁹ BA's Second Representations, para 5.28.

¹⁹⁰ BA's First Representations, paras 11.1-11.11.

¹⁹¹ BA's First Representations, paras 12.1-12.14.

claims in respect of the Commissioner's conduct in preparing the draft decision. In particular, BA builds upon its claims that the Commissioner's initial NOI was inadequately reasoned, and states that the Commissioner's draft decision bore little resemblance to the case put against BA in the NOI and is therefore unfair and contradicts the spirit of the statutory process.¹⁹²

7.126. The Commissioner does not accept any of these points.

7.127. First, the Commissioner is required to provide an adequately reasoned decision, which is intelligible and which conveys the reasons for the decision in such a way that enables the addressee to make representations and identify any errors of reasoning.¹⁹³

7.128. The NOI complied with those requirements. It is notable, in particular, that the NOI was sufficiently detailed to enable BA to submit 76 pages of closely argued representations, and additional annexes. The NOI (at paras 16 to 24) set out the Commissioner's understanding at that time of how the Attack occurred and the failures it disclosed – based on the information provided by BA – which enabled BA to make representations and provide further information. The Commissioner's reasons for the imposition of the penalty were set out at paras 27 to 35 of the NOI and relied and built upon the preceding paras. The fact that the Commissioner could, in BA's view, have produced a lengthier Notice is not a basis for the contention that the NOI was unlawfully or inadequately reasoned. Nor is it the case that a proposed greater penalty necessarily calls for a lengthier NOI.

7.129. BA gives a number of examples of what it purports to be inadequate clarity on the part of the Commissioner in the NOI, including alleged "*vagueness about the commencement and duration of any infringement by BA*"¹⁹⁴ and the reference to the total number of affected data subjects. Where appropriate and necessary, clarifications were provided in the draft decision and in this document.

¹⁹² BA's Second Representations, paras 2.9-2.12.

¹⁹³ See, for example, *R v London Borough of Croydon, ex p. Graham* (1993) 26 H.L.R 286; *R v Brent London Borough Council, ex p Baruwa* (1997) 29 HLR 915.

¹⁹⁴ BA's First Representations, para 11.17.

7.130. Second, BA's complaints about the Commissioner's internal record of decision-making are also not accepted, and it is unclear precisely what relevance these points are said to have to the matters under consideration. As would be expected, the Commissioner's internal decision-making processes develop and change, depending on the nature of any particular investigation. The reasons for the Commissioner's decision are fully recorded in this document.

7.131. Third, there is no obligation on the Commissioner to issue a penalty notice in precisely the same terms as the NOI. The Commissioner carried out a lengthy and detailed investigation into the Attack. The purpose of requiring the Commissioner to issue notices of intent is to permit consultation. Through issuing the NOI, BA was afforded the opportunity to use the consultation process to make meaningful representations which were capable of affecting the outcome of the investigation. BA was then provided with a second, additional, such opportunity through the Commissioner agreeing to consult again on the draft decision. As a result, BA has provided significant amounts of new information and documents to the Commissioner, and made detailed written representations. The Commissioner rightly took all of the material submitted by BA into account, which necessarily resulted in further clarity being brought to the circumstances of the Attack and a more detailed decision being produced.

7.132. Thus, while the draft decision and this Penalty Notice are more detailed, taking into account the new evidence and submissions received, this does not constitute an abuse of process or a breach of BA's rights of defence. The Commissioner's core concerns remain the same: BA did not have in place appropriate security measures to address the specific deficiencies that were exposed by the Attack. BA understood from the NOI, and the draft decision, the essential elements of the Commissioner's preliminary view that it had breached, in particular, Articles 5(1)(f) and 32 GDPR.

The Commissioner's conduct

7.133. The Commissioner has considered the claims made in chapter 12 of BA's First Representations about her conduct and that of her office.

7.134. First, there is no basis for BA's contention that the Commissioner has a closed mind. The Notice of Intent was expressly provided, in

accordance with the statutory scheme, to enable BA to make representations, which it has on two separate occasions. Those representations, and the further evidence BA has provided, have been taken into account, as is apparent from the content of this decision.

- 7.135. As to the fact of the draft decision being made public, the Commissioner made it clear in communications with BA's solicitors that a statement would be made by the Commissioner's office in response to BA's own statement to the markets. The press statement was a confirmation of the factual and regulatory position at that time. The Commissioner had carried out an "*extensive investigation*" and based on that investigation had "*issued a notice of its intention to fine British Airways...*". The statement refers to the "*proposed fine*" and states that the Commissioner "*will consider carefully the representations made by the company and the other concerned data protection authorities before it takes its final decision*".
- 7.136. The Commissioner has noted BA's complaints about the process that was followed and its wider concerns about natural justice. In the light of the express emphasis in the ICO press statement that no final decision had been made, and the process that has in fact been followed, the Commissioner does not consider that those complaints have any merit.
- 7.137. To the extent that any of these points are relied upon to allege actual or apparent bias on the part of the Commissioner, that allegation is rejected.¹⁹⁵ BA's claim that there has been any infringement of the right to a defence is not correct.
- 7.138. As to paras 12.12-14 of BA's First Representations, as explained above the Commissioner has not relied on the Draft Internal Procedure, in the light of BA's Representations.

¹⁹⁵ While paras 12.8-12.11 of BA's First Representations refer to such concerns being raised in other cases, and a concern on BA's [art that the ICO is not in a position to guarantee BA's right to natural justice, it was not specifically alleged that the Commissioner was actually biased or acting with apparent bias.

(9) The Panel of Technical Advisers

- 7.139. During the initial stages of her decision-making process, the Commissioner anticipated convening the Panel and gave an indication of the possible timetable which would apply in this regard in her letter dated 3 October 2019. That letter explained that the Panel "*may be convened before the ICO consults with the other concerned supervisory authorities.*"¹⁹⁶ However, the Commissioner subsequently considered the wider process and decided that she would not convene the Panel on the particular facts of this case, in particular as the draft of this Penalty Notice would be subject to the Article 60 GDPR process.
- 7.140. The Commissioner does not accept BA's argument that, in deciding not to convene the Panel, it has been deprived of an additional safeguard to protect controllers in complex cases through permitting expert input.¹⁹⁷ The correct starting point is that, even in cases concerning "*very significant penalties*", the RAP only provides that the Panel "*may be convened*". It has always been a matter over which the Commissioner has discretion. The Commissioner is not therefore obliged to convene a Panel. It is open to the Commissioner to keep the need for such a Panel to be convened, especially in the context of a new regime, under review. Given that in this case the notice will be submitted to the consistency mechanism enshrined under Article 60 GDPR, the Commissioner decided that further input from an additional expert panel was unnecessary.

(10) The Extension Agreement

- 7.141. On 23 December 2019, BA agreed to the Commissioner's request for an extension to the statutory timescales. However, BA states in its Second Representations that it was compelled to agree with the extension request because the Commissioner had mishandled the enforcement procedure and thereby subverted the statutory time limit.¹⁹⁸ BA also criticises the Commissioner for refusing to provide a copy of the draft decision without any agreement being in place to permit for consultation upon it.¹⁹⁹

¹⁹⁶ Emphasis added.

¹⁹⁷ BA's Second Representations, paras 2.13-2.16.

¹⁹⁸ BA's Second Representations, paras 2.17-2.30.

¹⁹⁹ BA's Second Representations, paras 2.17-2.30.

- 7.142. The Commissioner has already addressed the suggestions that the enforcement procedure was mishandled above.
- 7.143. Further, and in any event, the Commissioner does not accept that BA was compelled to accept the request for the extension.
- 7.144. First, as the Commissioner explained in her letter of 6 December 2019, she was willing to agree an extension, as permitted by the legislation, in order to allow for a further round of consultation in this case as sought by BA. The legislative scheme does not envisage consultation on a draft decision. But in the circumstances of this case, the Commissioner agreed that such consultation could take place if appropriate arrangements were put in place. There is nothing improper about a decision to permit further consultation if that can be accommodated within the statutory process.
- 7.145. Second, the Commissioner explained to BA in her letters of 13 and 18 December 2019 that it may be possible to complete the Article 60 process within a short time. However, if not, the provisions of the DPA must be read down and applied in a manner consistent with the GDPR, and in order to give effect to its provisions. That may involve reading down the six-month statutory deadline (or, if necessary, the Commissioner would issue a fresh notice of intent) in order to allow time for the mandatory EU process, which could be of considerable length, depending on the facts of the case.
- 7.146. Third, BA's submissions proceed on the basis that it has been deprived of an important procedural safeguard as a result of the extension. Yet, Parliament made explicit provision for the Commissioner to agree an extension with controllers. The agreement of such an extension can permit the EU-law mandated process to be accommodated, as Parliament intended. Further, as outlined above, the extension has provided BA with an additional opportunity for consultation on the draft decision. Contrary to BA's submissions,²⁰⁰ it has not therefore suffered severe prejudice as a result of the consultation and decision-making processes being extended.

²⁰⁰ BA's Second Representations, para 2.27.

- 7.147. Fourth, contrary to BA's submissions,²⁰¹ there was no obligation on the Commissioner to conduct a further round of consultation irrespective of whether an extension was agreed. The legislation does not envisage or require such further consultation. BA's criticisms of the Commissioner's position that she could not share the draft decision before an extension was agreed are misconceived. Given that the legislative regime does not envisage such consultation, it could not be accommodated without agreeing an extension. It was also not necessary for BA to see the draft decision (and thereby presumably take up the opportunity to make submissions in response to it in any event) before deciding whether it agreed to an extension, accommodating its request for further consultation and the Article 60 process.
- 7.148. Fifth, as a matter of fact BA did provide significant new information, and adduced detailed written submissions, during the course of the decision-making process. Given the complexity of the case and matters under investigation, it can be no criticism of the Commissioner that she has taken time carefully to consider all material put before her, and she has offered additional opportunities for consultation in this case.
- 7.149. In short, the statutory deadline is not absolute. Parliament provided expressly for an extension mechanism. The Commissioner does not, therefore, accept that in agreeing to an extension BA was 'forced' to forego important procedural safeguards envisaged by statute.²⁰² Instead, by agreeing to the extension, BA chose to obtain the benefit of being able to make a second round of representations.
- 7.150. Finally, BA has no basis to question the integrity of the Article 60 process, the arguments advanced at paragraph 2.28 of BA's Second Representations are speculative and without any reasonable basis.
- (11) The Commissioner's compliance with her statutory obligations
- 7.151. The Commissioner's conduct of this matter has been transparent, accountable, proportionate, and consistent. As to the specific claims made by BA at paragraphs 6.1 and 6.2 of its Second Representations in this regard:

²⁰¹ BA's Second Representations, paras 2.25-2.27.

²⁰² BA's Second Representations, para 2.24.

- a. The Commissioner, taking into account BA's First Representations, places no reliance upon her Draft Internal Policy. The factors which were taken into account when calculating the proposed penalty sum have been extensively, fully, and entirely transparently set out in this Penalty Notice (and the earlier draft decision, in response to which BA has made full representations).
- b. BA, in both of its Representations, has provided detailed representations which comprehensively challenge the Commissioner's decision to impose a penalty and the calculation of the proposed penalty. In these circumstances, and for the additional reasons given above, the Commissioner does not accept that BA cannot effectively challenge the Commissioner's penalty calculation.
- c. The penalty is entirely proportionate, and the Commissioner was entitled to take into account BA's turnover in ensuring that the proposed penalty was dissuasive.
- d. The Commissioner is obliged to act consistently with her previous enforcement action only where there are comparable cases (both in terms of their facts and the applicable legal regime). The Commissioner has considered the comparators which BA has cited, and – for the aforementioned reasons - she does not accept these reveal an inconsistent approach. For the reasons given above, the Commissioner has not acted inconsistently with any previous public statements. The fact that the Commissioner took into account BA's Representations with respect to the Draft Internal Procedure and changed her approach, is evidence of the effectiveness of the procedural safeguards built into regulatory decision-making, rather than an example of an inconsistent approach. With regards to convening the Panel, this has been addressed above.

7.152. With regards to paras 6.3-6.5 of BA's Second Representations, the Commissioner accepts that pursuant to section 108 of the Deregulation Act 2015, she must have regard to the desirability of promoting economic growth, and thereby exercise her regulatory functions only where needed and where proportionate. The Commissioner notes that the list of factors referred to by BA are only

described by the relevant statutory guidance at para 4.3 as “*indicators*” that the duty under section 108 has been complied with. They are not intended to be or described as a list of exhaustive factors which must – in all circumstances – be taken into account by the Commissioner to demonstrate compliance with the duty under section 108. In this regard, the Commissioner notes that:

- a. she is required, by Article 83(1) GDPR, to ensure that any penalty imposed is proportionate and has done so;
- b. Article 83(2) GDPR requires the Commissioner to take into account the nature and gravity of the infringement and the degree of responsibility of the controller (in relation to which the Commissioner has taken into account the steps BA took to achieve compliance and the reasons for BA’s failures);
- c. Article 83(2) GDPR requires the Commissioner to take into account the degree of BA’s cooperation with the Commissioner and the steps which BA took to mitigate the damage suffered by data subjects. The Commissioner has thereby considered the steps BA took towards achieving compliance;
- d. The likely impact of any penalty on BA, including in terms of the economic cost, was considered when the Commissioner considered any mitigating factors pursuant to Article 83(2) and also when specifically considering financial hardship under Step 5 of the penalty calculation under the RAP;
- e. The Commissioner was obliged to ensure that any penalty imposed would be dissuasive, both in respect of BA but also others, pursuant to Article 83(1) of the GDPR and under Step 4 of the penalty calculation in the RAP.

7.153. The Commissioner has, therefore, had regard to the indicative factors listed within the relevant statutory guidance.

7.154. The Commissioner also notes that the obligation under section 108 is not designed “*to legitimise non-compliance and its purpose is not to achieve or promote economic growth at the expense of necessary protections.*” Rather, “*the purpose is to ensure that specified regulators give appropriate consideration to the potential impact of their activities and their decisions on economic growth, both for*

individual businesses and more widely for sectors or groups they regulate, alongside their consideration of their other statutory duties" (see para 1.5 of the statutory guidance). The Commissioner has not identified any risks to economic growth in the exercise of her regulatory functions in this matter, nor has BA put forward any cogent case to suggest that there will be any such risk. BA refers to the use of turnover as a "core metric" as being contrary to the promotion of economic growth, however this is entirely misguided. Turnover is an important metric because it ensures that, for similarly serious infringements, larger companies are issued with larger penalties than smaller penalties. This approach is inherently proportionate and cannot pose any risk to economic growth.

8. HOW THE PENALTY IS TO BE PAID

- 8.1. The penalty must be paid to the Commissioner's office by BACS transfer or cheque.
- 8.2. The penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

9. ENFORCEMENT POWERS

- 9.1. The Commissioner will not take action to enforce a penalty unless:
 - the period within which a penalty must be paid has expired and all or any of the penalty has not been paid;
 - all relevant appeals against the penalty notice and any variation of it have either been decided or withdrawn; and
 - the period for appealing against the penalty and any variation of it has expired.
- 9.2. In England, Wales and Northern Ireland, the penalty is recoverable by Order of the County Court or the High Court. In Scotland, the penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 16th day of October 2020

Signed:

Elizabeth Denham
Information Commissioner

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 162(1) of the Data Protection Act 2018 gives any person upon whom a penalty notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.
2. If you decide to appeal and if the Tribunal considers:-
 - a) that the notice against which the appeal is brought is not in accordance with the law; or
 - b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.
3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

General Regulatory Chamber
HM Courts & Tribunals Service
PO Box 9300
Leicester
LE1 8DJ

 - a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.
 - b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.
4. The notice of appeal should state:-

- a) your name and address/name and address of your representative (if any);
 - b) an address where documents may be sent or delivered to you;
 - c) the name and address of the Information Commissioner;
 - d) details of the decision to which the proceedings relate;
 - e) the result that you are seeking;
 - f) the grounds on which you rely;
 - g) you must provide with the notice of appeal a copy of the penalty notice or variation notice;
 - h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.
5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.
6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 162 and 163 of, and Schedule 16 to, the Data Protection Act 2018, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).

Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:UK:OSS:D:2020:147

Background information

Date of final decision:	16 October 2020
Date of broadcast:	16 October 2020
LSA:	UK
CSAs:	All SAs
Legal Reference:	Personal data breach (Articles 33 and 34), Security of processing (Article 32)
Decision:	Administrative fine
Key words:	Administrative fine, Data security, Hacker attack, Personal data breach, Credentials

Summary of the Decision

Origin of the case

On 22 June 2018, the unidentified attacker gained access to controller's IT systems via CAG (a tool that allows users to remotely access a network) and maintained this ability to access undetected until 5 September 2018.

After gaining access to the wider network, the attacker traversed across the network. This culminated in the editing of a Javascript file on the controller's website. The edits made by the attacker were designed to enable the exfiltration of cardholder data from that website to an external third-party domain, which was controlled by the attacker.

The controller was alerted by a third party about the exfiltration of personal data from the controller's website and then notified the LSA about the attack on 6 September 2018.

The controller estimated that 429,612 data subjects were affected. The affected categories of personal date were: username and passwords of contractors, employees and members of the Executive club, customer names and addresses, unencrypted payment card data including card numbers, and CVV numbers and expiry dates.

The controller took immediate measures to mitigate and minimise any damage suffered by the data subjects by implementing remedial measures, including notifying banks and payment schemes, the data subjects and data protection regulators; cooperating with regulatory and governmental bodies; and offering a reimbursement to all customers who had suffered financial losses as a direct result of the theft of their card details.

The controller also implemented a number of remedial technical measures to reduce the risk of a similar attack in future.

Findings

The LSA found that the controller failed to process the personal data of its customers in a manner that ensured appropriate security of the data, including: protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures, as required by Article 5(1)(f) and by Article 32 GDPR.

The LSA concluded that there are a number of appropriate measures that the controller could have considered to mitigate the risk of an attacker being able to access the controller's network. The LSA considered that each step of the attack could have been prevented, or its impact mitigated, by the controller's implementing one or more of those appropriate measures that were open to controller. The LSA also considered that, had the controller performed more rigorous testing or internal penetration tests, it would have likely detected and appropriately addressed many of the data security problems identified.

Decision

The LSA concluded that the infringements constitute a serious failure to comply with the GDPR. The LSA decided to impose on the controller an administrative fine of £20 million, after having taken into account a range of mitigating factors and the impact of the Covid-19 pandemic.

Summary Final Decision Art 60

Complaint

Compliance order to controller

Background information

Date of final decision:	17 May 2019
LSA:	BE
CSAs:	NL, SE
Legal Reference:	Right to erasure (Article 17), Transparent information, communication and modalities for the exercise of the rights of data subjects (Article 12)
Decision:	Compliance order to controller
Key words:	Right to erasure, Exercise of the rights of the data subjects

Summary of the Decision

Origin of the case

The complaint concerned the failure of the controller to comply with the request of a data subject concerning the exercise of his right of erasure. After two submissions of the webform in order to have his data removed, the complainant also sent e-mails with the same request on 28/06/2018. The complainant still did not receive any reply and asserted that the controller did not respond within a month following the request.

Findings

The controller has failed to comply with the request of the data subject, thus violating its obligations under Article 12.3 GDPR. The LSA considers that the deadline to answer the request "has been exceeded at all levels".

Decision

The LSA decided to order the controller to comply with the data subject's request concerning the exercise of the right of erasure.