

Summary Final Decision Art 60

Complaint

Administrative fine, Compliance order

EDPBI:ES:OSS:D:2021:263

Background information

Date of final decision:	1 July 2021
Date of broadcast:	3 August 2021
LSA:	ES
CSAs:	DE-BE, DE-MV, DE-NW, DE-SL, DE-SN, DE-RP, FR, IT, NO
Legal Reference:	Principles relating to processing of personal data (Article 5), Lawfulness of processing (Article 6), Right to transparent information, communication and modalities for the exercise of right of the data subject (Article 12), Information to be provided where personal data are collected from the data subject (Article 13), Right to object (Article 21)
Decision:	Administrative fine, Compliance order
Key words:	E-commerce, Transparency, Principles relating to processing of personal data, Lawfulness of processing, Data subject rights, Right to be informed, Right to object

Summary of the Decision

Origin of the case

On 15 October 2018, a data subject residing in Germany lodged a complaint with the DE-BE SA against a website selling furniture and decorative accessories in Germany. This complaint alleged a lack of information on data protection and missing cookie warnings on the website, as well as the refusal by the company to issue an invoice unless buyers provide their tax identification number. As the company operating these websites was found to be established in Spain, the ES SA has been identified as the lead supervisory authority (LSA).

Findings

The LSA found that the privacy policy of the controller's website was difficult to read due to a large number of grammatical and spelling errors, and that its structure was confusing. As a result, the LSA found that the privacy policy violated Article 12 (1) GDPR with regard to the obligation to provide information to data subjects in a concise, transparent, intelligible and easily accessible form.

Additionally, several shortcomings were identified by the LSA as to the content of the controller's privacy policy, resulting in a violation of Article 13 GDPR (Information to be provided where personal data are collected from the data subject).

In particular, the LSA ruled that since the information concerning the right to object under Article 21 (1) GDPR is drafted in a confusing manner, this made it more difficult for data subjects to exercise their right to object to processing of their data for direct marketing purposes. As a result, an infringement of Article 21 (4) GDPR (Right to object) was found by the LSA.

Finally, the LSA considered that, as the complainant had the right to request a simplified invoice without being asked for an identification number to be issued, the controller infringed Article 6 (1) and, consequently, the principle laid down in Article 5 (1) (a) GDPR.

Decision

In view of the above, the LSA imposed to the controller an administrative fine of 6,000 euros for infringements of Articles 5(1)(c), 6(1), 12, 13 and 21 GDPR.

The controller was given three months to align its privacy policy with Articles 12 and 13 GDPR, as well as to stop requesting the customer's tax identification number unless it obtained a valid consent or it is required by law to process this data.

File No: PS/00003/2021

IMI Reference: A56ID 113249- Case Register 123773

FINAL DECISION ON PENALTY PROCEEDINGS

Of the proceedings conducted by the Spanish Data Protection Agency and on the basis of the following

FACTS

FIRST: On 03 March 2020, via the ‘Internal Market Information System’ (hereinafter IMI), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), which aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information, the Spanish Data Protection Agency (AEPD) received a complaint dated 23 December 2018 from [REDACTED] (hereinafter the complainant) to the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP). This complaint is transmitted to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the General Data Protection Regulation or GDPR), taking into account its cross-border nature and that this Agency is competent to act as lead supervisory authority.

The complaint is made against *Michael Page International* on the following grounds:

- . The complainant, a Dutch citizen, opened an account in the Dutch version of Michael Page International’s web portal, accessible at the URL “www.michaelpage.nl”, and in March 2018 sent a Curriculum Vitae (CV) for a job offered by the Dutch branch of the PageGroup group. A few months later, she requested access to her personal data via the email address indicated in the Privacy Policy of the web portal, “gdpr@pagegroup.eu”.
- . In response to the above-mentioned access request, the responsible entity initially required the complainant to provide two out of three categories of identification documentation (passport, national identity card or driving licence), showing the date of birth; social security or national insurance card and invoice for energy supply or water for less than 3 months. However, following the applicant’s protest, which considered the request for documentation to be excessive, Michael Page International corrected and requested only a copy of the identification document on both sides.
- . The complainant considers that there is no reason to request this identification information, which was not required to open an account on the web portal, or to submit a CV for the purpose of applying for a job. The complainant considers that authenticated access to the account, which is still active, should be sufficient to understand the exercise of the right of conformity and the identity of the applicant in a system such as that used

by the controller, based on the use of a private account.

The complaint provided a copy of the complainant's correspondence with the controller following the request for access, dated 28 September 2018, which was also accompanied. This correspondence is set out in Facts 4 to 9.

The documentation relating to this complaint was supplemented by voluntary assistance in IMI, sent by Autoreit Persoonsgegevens on 12 May 2020, incorporating the consultation which the Dutch authority made to the establishment of the PageGroup group in the Netherlands (Michael Page International — Nederland Bv), in the Dutch language, on decision-making relating to the means and purposes of the processing of personal data concerning residents of the Member States.

The reply given by that establishment to the abovementioned consultation, in English, states that, although the headquarters of the group are located in the United Kingdom, the department responsible for managing access requests for continental Europe is the Legal Compliance Team, located at the Centre for Shared Services in Barcelona (Spain). The postal address of that department is indicated in the Privacy Policy of the Dutch version of the Responsible Officer's website, accessible in the URL "<https://www.michaelpage.nl/en/privacy>".

According to that reply, the Spanish establishment of the group of companies would be the main establishment within the meaning of the definition in Article 4 (16) of the GDPR. Thus, in accordance with Article 56 (1) of the GDPR, on 21/05/2020, the AEPD declared itself competent to act as lead supervisory authority (LSA).

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, in addition to the supervisory authority which reported the case (the Netherlands), Belgium, Ireland, Poland, Italy, Hungary, Portugal, Cyprus and Austria, as well as the German regional authorities of North Rhine-Westphalia, Rhineland-Palatinate, Mecklenburg-Western Pomerania, Berlin and Bavaria Private Sector, have declared themselves concerned in the present proceedings.

SECOND: In accordance with the procedure laid down in national legislation (Article 64 (3) of the Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights — LOPDGDD), on 11 June 2020, the AEPD transmitted the complaint to the Spanish establishment of the PageGroup group based in Hospitalet de Llobregat, namely the company PAGE GROUPEUROPE, S.L. ('PAGE GROUP EUROPE'). in order to demonstrate within one month that it responded to the complainant's request, provide information on the reasons for the incident and set out the measures taken to avoid similar situations.

In response to that request, PAGE GROUP EUROPE provided the following communications with the complainant:

. They explain that they are a company that is part of a business group dedicated to human resources services, namely recruitment. For this reason, they process personal data of a high number of candidates in many countries of the world, with the exercise of rights by candidates being very common. In order to process the relevant requests, in compliance with its duty of confidentiality and secrecy, it has implemented a strict identity

verification process to ensure that candidates' personal data are not transferred to third parties, that they may have obtained the access credentials of persons registered in their systems for the purpose of deleting their identity and making the application on their behalf, through phishing or social engineering attacks.

. In the particular case of the complainant, they have not sought to hinder the exercise of her rights, but rather to protect her personal data. In fact, as is apparent from the communications submitted by the interested party, the opportunity was offered to provide a copy of her ID as an alternative to the initial procedure, which required the production of two documents proving identity, without any reply from the complainant.

. It adds that "*it has abolished the procedure whereby two out of three categories of identification documentation were requested. At present, PAGE only requests an identification document and also offers alternatives to interested parties, such as signing by means of an electronic certificate, face-to-face care in any office of PageGroup or any other means which the person concerned considers appropriate*".

On this point, it provides a copy of the 'Reply Models' currently used to verify the identity of the parties concerned. The first of these requests the person concerned to copy the identity card or EIN, passport or driving licence with date of birth, any of them; attention is also drawn to the possibility of using alternative means, should the person concerned prefer not to send such documents. The second model refers to such alternative means, such as the presence in a Group office or the sending of a document signed by means of an electronic certificate.

Subsequently, by letter of 14 August 2020, the Agency asked PAGE GROUP EUROPE '*a copy of the reply to the request for access raised by the complainant, since its identity has been proven through the complaint procedure initiated before the supervisory authority of the Netherlands and continued at this Agency*'. Following this request, the aforementioned entity responded to the complainant's request for access and provided the Agency with a copy of the communication dated 27 August 2020 informing the Agency of the aspects of the processing provided for in Article 15 of the GDPR, as well as the annex containing the complainant's personal data in its possession. The reply to this Agency states that the information was sent by e-mail.

THIRD: Having reviewed the reply provided by the company complained of, as set out in the previous facts, the Agency found that, at present, the procedures followed by PAGE GROUP EUROPE for the attention of data protection rights, in relation to the identification of applicants, comply with the applicable legislation. Considering that the documents it manages as a company active in the human resources sector contain a lot of personal information, the requirement to request additional identification documentation in order to comply with a request for access was considered reasonable, taking into account the 'phishing' or social engineering attacks that may occur, as well as unauthorised accesses that suffer from email accounts worldwide.

In addition, it was taken into account that, following the intervention of this Agency, the complainant's request for access was granted.

Consequently, it was considered that there was no evidence of an infringement and that no further action was necessary or that further action was required, so that, on 10

November 2020, a draft decision to discontinue proceedings was issued.

FOURTH: On 10 November 2020, the draft decision was incorporated into the IMI system so that the authorities concerned could make their views known.

At the end of the deadline, the Data Protection Authorities of Portugal (CNPD) and Berlin (The Berlin Commissioner for Data Protection and Freedom of Information -Berlin DPA) raised objections to the above-mentioned draft decision.

The CNPD states that PAGE GROUP EUROPE has implemented a rights clearance procedure whereby it requests identification documentation in any case, without taking into account the circumstances of each request, and has not specified that in the case of the complainant it had doubts regarding her identity. It considers that the aforementioned entity has failed to comply with Article 12 (2) of the GDPR, which obliges the controller to facilitate the exercise of the rights, unless it is unable to identify the applicant, in which case Article 12 (6) of the GDPR allows additional identification information to be requested.

Also understands from the CNPD that the procedure followed by the responsible entity does not protect the data of the applicants, as the processing of the required identification documents increases the risks for those concerned (e.g. possible use for identity theft); it also takes into account that this documentation was not required from the complainant to open an account or send a CV. The Portuguese authority believes that this violates the principle of minimisation (Article 5 (1) (c) GDPR), privacy by default and by design (Article 25 GDPR) and security measures (Article 32 GDPR).

The CNPD advocates a less intrusive way of verifying the identity of the applicant (e.g. electronic identification or sending the request via the user account together with an additional authentication factor submitted via another channel).

Berlin DPA, for its part, also finds an infringement of Article 12 (2), (3) and (6) of the GDPR for reasons similar to those put forward by the Portuguese authority. Considers that additional information should only be requested if there are doubts as to the identity of the data subject, requesting necessary and appropriate information for such verification, on the basis of the applicant's available data; it does not share the justification put forward regarding the possible risk of emails being buried. Furthermore, given that the ID card was not required to register, Berlin DPA considers that it cannot be used for verification purposes, or at least would not be the most appropriate form, and agrees with the complainant's assessment that registered access to the private account would be more than sufficient.

Berlin DPA points to a possible infringement of Article 12 (3) GDPR because the controller did not reply within one month of the submission of the request.

It objects to the rejection of the complaint and considers it appropriate to identify infringements and take corrective measures against the controller so that it can correct its procedures in order to avoid jeopardising the rights of other applicants or the obstacles to their exercise.

FIFTH: The objections raised by the data protection authorities referred to in the previous

Facts have been taken into consideration and, on 11 December 2020, the complaint communicated by the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) was declared admissible, without prejudice to what may be determined in the course of the processing of the complaint.

SIXTH: On 26 February 2021, the General Subdirectorate of Data Inspection accessed the website 'www.michaelpage.es' and obtained information on PageGroup.

The corporate information in the section '*What are we*' on that website states:

"PageGroup is the leading international consultant in the selection of qualified, middle and senior managers on a temporary and indefinite basis. It was established in the United Kingdom in 1976 and has been listed on the London Stock Exchange since 2001. With a network of 140 own offices, we operate in 36 countries around the world. In Spain, we offer coverage at national level with physical offices in Madrid, Barcelona, Valencia, Seville, Bilbao and Zaragoza through which we provide recruitment services and career opportunities at local, regional and global level. Within the group we have different brands, each expert on its market".

The website "www.pagegroup.com" is also accessed and the annual report for 2019 ("*Annual Report 2019*") is obtained. According to the information contained in this document, which is incorporated into the actions, PageGroup made a gross profit of GBP 855,5 million in 2019 and an operating profit of GBP 146,7 million.

According to the information in the Central Commercial Register concerning PAGE GROUP EUROPE, the 'subscribed capital' amounts to 60 000,00 EUR.

Information on PAGE GROUP EUROPE is available on the website "axexor.es", which shows a sales volume of more than 34 million EUR. The number of employees is 376.

SEVENTH: On 02 June 2021, in accordance with Article 64 (2) (third subparagraph) and (3) of the LOPDGDD, a revised draft decision to initiate penalty proceedings was issued on the basis of the complaint received via the IMI system, as set out in the First Fact. This revised draft decision takes into account the objections set out in the Fourth Fact.

In accordance with the procedure laid down in Article 60 of the GDPR, on 13 March 2020, the aforementioned revised draft decision to initiate penalty proceedings was sent via the IMI system to the supervisory authorities concerned, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate penalty proceedings would be adopted.

None of the supervisory authorities concerned has raised any objection to the revised draft decision to initiate penalty proceedings adopted by the AEPD, and it is therefore understood that there is agreement on it.

EIGHTH: On 29 June 2021, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against PAGE GROUP EUROPE, in accordance with Articles 63 and 64 of the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), for the alleged infringement of Articles 5.1 (c) and 12 of the GDPR, as set out in Articles 83.5 (a) and (b) of the same Regulation, respectively; establishing that the fine that might be applicable would amount to a total of 300,000 EUR (250,000 EUR for the infringement

of Article 5 (1) (c) and 50,000 EUR for the infringement of Article 12, both of the GDPR), without prejudice to the outcome of the proceedings.

The same decision initiating the procedure stated that the alleged infringements, if confirmed, could lead to the imposition of measures, in accordance with the provisions of Article 58 (2) (d) of the GDPR.

NINTH: Having notified the above-mentioned decision to initiate proceedings and extended the deadline for submitting allegations, PAGE GROUP EUROPE submitted a letter dated 21 July 2021, requesting that the AEPD's initial approach be maintained and that the penalty proceedings be closed or, in the alternative, that the proposed fine be reconsidered, taking into account the reprimand provided for in the legislation. In summary, that entity bases its request on the following considerations:

1. As a preliminary point, it highlights the good faith and willingness to comply which has governed its action and the internal policies applied, and expresses its intention to provide more information and clarity with its arguments on the case, despite the fact that it entails a waiver of the application of the reduction of the proposed penalty, in the belief that they have followed the recommendations of the authorities and that their motivation was only an excessive zeal in the protection of personal data for not giving data to a person other than the beneficial owner of the data. It adds that the question raised concerns an interpretation of the provision, which is still only recently applied.

2. It takes the view that it is contradictory to state in the legal bases of the opening agreement that the outcome of the transfer procedure '*was not satisfactory*', when it is stated in the Second and Third Fact that the requested party responded to the request for access made by the complainant, that the procedures currently applied for the attention of rights comply with the applicable legislation or that the request for additional identification documentation was considered reasonable, concluding that there were no indications of infringement and that it was not necessary to adopt additional measures.

On this basis, it requests that the documents in the file be reviewed again, clarifying in this regard, in the event that the statement is motivated by the absence of a reply to the Dutch authority's first request, that in June 2019, access to dpo@page.com was granted to persons in the Legal Compliance Team on a temporary basis, on the ground that the person providing DPD services would leave the company at the beginning of July 2019 and until another person took up those duties, although for some technical reason the connection was only effective at the end of August, without it being possible to recover the emails received in the meantime.

As soon as it became aware that the Dutch Data Protection Authority (Autoreit Persoonsgegevens -ap) had sent 2 emails on 23 July 2019, it contacted it, although there is no record of having received a reply.

Subsequently, on 30 August 2019 Autoreit Persoonsgegevens sent a letter directly to Michael Page International — Nederland Bv, to which it replied on 27 September 2019.

3. In relation to the alleged infringement of Article 5 (1) (c), it highlights the review of its internal policies carried out in 2016-2018 in order to bring them into line with the new legislation, on which there were no guiding criteria for interpreting novel concepts such

as the principle of data minimisation or privacy by design or by default. It therefore tried to combine measures and recommendations that remained in force with an interpretation of the new legislation aimed at strict compliance with it.

This process included reviewing and updating the procedure for dealing with the rights of those affected, with three key measures, such as the appointment of a DPO and the centralisation of that procedure in PAGE GROUP EUROPE, which was granted the power to decide whether the request for the exercise of rights was valid or required an application for an identification document in order to verify the identity of the person concerned and to process the exercise of rights.

According to the internal criteria followed, no identity document was requested in the exercise of rights relating to requests for rectification, erasure or forgotten, limitation or objection, but in cases where the exercise of the right of access or portability was requested, which involve the provision of curriculum vitae data that may contain relevant information. It was intended to confirm identity in order to protect those affected from possible identity theft and it was understood that the possession of an official document matching the name and surname with the information available in the database was a credible evidence that the same person was involved.

It then pointed out that few requests had been received since May 2018 and provided details of the access requests processed since that date:

- . 2018: 50 requests for access, representing 1.66 % of the total
- . 2019: 62 requests for access, representing 1.56 % of the total
- . 2020: 55 requests for access, representing 1.65 % of the total
- . 2021: 28 requests for access, representing 1.63 % of the total

On the other hand, as regards Berlin DPA's interpretation of the appropriate means of verifying the identity of the data subjects exercising a right, the requested body considers that those assessments derive from local idiosyncracy and may be motivated by historical issues, inherited from previous local regulations, cultural or compliance aspects, which will be defined and standardised over the coming years.

After analysing the German Identity Document Act ('Personalausweisgesetz'), it requests that the facts and conclusions be reviewed in the light of the following circumstances:

— The presentation of a copy of the identity card was deemed necessary only in the requests for the exercise of the right of access and portability as there was an increased risk of sharing data with a person other than the beneficial owner of the data because of the reasonable doubts about the identity of the person arising from phishing and forging of usual practices and a real concern in the recruitment sector; Page has suffered several attempts of cyber fraud by third parties to pass through their employees in an attempt to obtain personal data from data subjects. Due to distance, it is not only possible to display the identity card by the person concerned at the company's registered office or at a branch, and it was therefore considered necessary to request a digital copy of the identity card for this purpose;

— Only the legal compliance team had access to such a document, which it used only to verify identity, not including the document on the file of the person concerned or carrying out any further processing;

— Only the first name and surname were checked for identification purposes. The other data, according to that German law, could and should have been crossed out by the data subject at the time of shipment (for example, access and serial numbers, nationality, date of birth, stature, colour of eyes, photograph and machine-readable zone). The German legislation already provides for other information to be obscured. We therefore consider that it is common practice in Germany to request this type of documentation for verification purposes.

Furthermore, the requested entity claims to have studied that the Dutch authority has been active as regards the illegal processing of the BSN (Personal Identification Number) and has taken several enforcement measures before the entry into force of the GDPR, including:

- . Airbnb unlawfully dealt with the BSN (through complete copies of the identity documents) and the DPA published its findings in this regard. No fine was imposed and no investigation report was published after Airbnb changed its operations.
- . A freight company called Nippon Express processed complete copies of the identity documents and BSN of the lorry drivers entering the premises to collect the cargo. This was illegal according to the Dutch DPA and published an investigation report without penalising the company after changing its procedures.

As can be seen, and will be further developed, the requested entity does not derive any benefit from extending or allegedly hindering the exercise of a right which entails the provision of information to the data subject. This is not a departure from a service or an objection to a particular treatment that the entity had an interest in maintaining.

That measure was understood to be proportionate by assessing, on the one hand, the damage that could be caused by providing curriculum vitae information to third parties other than the holder with regard to the ‘inconvenience’ which may involve sending/displaying an identity document, which most citizens are already scanned.

On the basis of this, it requests that the arguments of Berlin DPA and the CNPD that changed the AEPD approach, which decided to close the procedure as it did not assess intent in the action carried out by PAGE GROUP EUROPE, be reconsidered because of the lack of profit and the improvement implemented.

4. The processing carried out, consisting of verifying the match of the first name and surname of the document with those in the database, complies with the principle of minimisation (recital 39 GDPR): the requested document was suitable to allow for such verification; it is relevant because it does not involve a disproportionate effort on the part of the operator to submit it; the processing of that document was limited to what was necessary in relation to the purposes for which it was processed, without adding any additional information contained therein to the data subject’s file and without any further processing of the document. Similarly, the concept of restriction of access was incorporated, since that data was processed only by the Legal Compliance Team, which did not process that document subsequently. It therefore does not represent an additional risk for the data subject.

Considering this lack of further processing and the fact that the processing carried out was very limited in time, as was the access to the information in question, the requested entity considers that recital 156 of the GDPR is complied with: *‘The conditions and safeguards in question may include specific procedures for the exercise of those rights’*

by data subjects if it is appropriate in light of the purposes for which the specific processing is carried out, together with technical and organisational measures aimed at minimising the processing of personal data having regard to the principles of proportionality and necessity'; it was considered, after consideration, that this measure was necessary, proportionate and appropriate to protect the rights of the person concerned.

5. With the aforementioned requirement, the respondent did not attempt to extend, hinder or hinder the exercise of rights by the person concerned, nor did it benefit from that practice, which required a specific procedure to be designed and resources invested in management and monitoring. If, finally, it is established that such a procedure was not properly designed, the only thing that can be attributed to it is an excess of the intention to comply with it, in order to ensure that no data was handed over to a person other than its holder, but not that this request was intended to hinder the exercise.

The entity considered as likely a scenario of identity theft, in which one person would access the email or account access keys of another person, in order to obtain the data from that account, and therefore considered an alternative means other than the usual authentication of the user.

6. With regard to the alleged infringement of Article 12 of the GDPR, the respondent puts forward arguments seeking to respond to the arguments put forward by the data protection authorities of Berlin and Portugal, but do not start by insisting that the entity is alert to access requests because they are not frequent in its activity, since it is the data subjects themselves who directly provide their personal data and have the information available to them in their personal area.

With regard to Berlin DPA's statement, which does not share the potential risk of emailing e-mail addresses, the respondent shows that there are studies and statistics that demonstrate the hypothesis that the request for the right of access to the GDPR may be a point of vulnerability to social engineering attacks.

And adds:

"To cite some of these studies, James Pavur (DPhil researcher Oxford University) and Casey Knerr (Security Consultant Dionach LTD) state in their publication "GDPArrrr: Using Privacy Laws to steal Identities":

"In this work, we have raised the hypothesis that the right to request access can be a point of vulnerability to social engineering attacks. Through an experiment covering 150 organisations, we demonstrated the feasibility in the real world of such attacks. We found that a large proportion of organisations do not adequately verify the origin identity of access requests and that, as a result, deeply sensitive information can be acquired repeatedly and scalable by social engineering. We suggest a number of corrective measures focused on individuals, businesses and legislators to help mitigate these attacks.

(...)

Requesting a photo identification issued by the government is probably the most robust way to prevent this attack. However, organisations that are not able to adequately protect this data, or to verify its authenticity, should consider subcontracting these services to a third party.

Companies should also regularly assess their process of requesting access from the subject in search of vulnerabilities and train individual representatives of the service in detecting and responding to such attacks. The addition of malicious access requests...".

Recital 64 GDPR itself states that '*The controller should use all reasonable measures to verify the identity of a data subject who requests access*'. Furthermore, Article 12 (6) GDPR provides 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*'.

In Spain, the need to provide the identity card or equivalent document by the data subject was provided for in Article 25 of the repealed, almost entirely, Royal Decree 1720/2007. That article stated that notification of the exercise of rights to the controller should be accompanied by a photocopy of the person's national identity card, passport or other valid document identifying him.

The Spanish Data Protection Agency itself (AEPD), in its '*Guide for the Citizen*', states that '*if the controller has doubts as to the identity of the data subject, it may request additional information in order to confirm it, such as a photocopy of the ID card, passport or other valid document*'.

In addition, the forms that the AEPD designed as models for the exercise of rights and which it presents as templates for use by citizens include the following instruction:

'2. A photocopy of the D.N.I. or equivalent document proving identity must be provided and considered valid in law, in cases where the person responsible has doubts as to his identity. In the event of legal representation, the identity card and document certifying the representative's representation must also be provided'.

This is therefore a common practice, at least in Spain, the residence of our company, which does not violate the principle of data minimisation, which requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Claims that it made an error in explaining the duty clearance procedure implemented, which led to the CNPD's indication of the request for '*identification documentation in any event, without taking into account the circumstances of each application, and did not specify that in the case of the complainant it had doubts regarding its identity*'; it points out that this internal procedure (attached as an annex) specifies that the identity of the applicant is checked in case of reasonable doubts about it ('Request valid'), in which case it is verified by requesting an ID validation.

This measure was taken in compliance with the principles of data protection by design and by default, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing, as well as the risks of varying likelihood and severity of the processing for the rights and freedoms of natural persons, taking into account the amount of personal data collected (identification card), the extent of their processing (verification of consistency with the data of the data subject available), their storage period (erased immediately after verification) and their accessibility (only the Legal Compliance Team, and ultimately the DPO had access).

With regard to the increased risks for those affected, also highlighted by CNPD, it reiterates once again that the identity document was required only in the exercise of the right of access, not in other rights, and that all the necessary technical and organisational

measures were put in place so that, once the check had been carried out, the document received was deleted.

7. Stresses once again the good faith and degree of collaboration shown, having modified the internal rights management procedure as follows:

The Legal Compliance Team validates the identity of the applicant, which is considered validated if the first name, surname and e-mail match those in the database. Additional information is requested only when we have reasonable doubts about the identity of the applicant.

The criteria for determining whether there are doubts about the identity of an applicant are:

I. Receiving the access request from a valid email address recorded in the database is sufficient to verify the identity of the applicant.

An email response is sent to the requester confirming receipt of his/her right of access.

II. If there are reasonable doubts about the identity of an applicant, for example because there are several persons with the same name, or there are duplications/doubts about the e-mail address, additional information is requested to verify his/her identity by email, explaining to the applicant the existence of doubts about his/her identity and the need to confirm it. Only information that is already in the applicant's profile, e.g. postcode or the last 3 digits of the applicant's telephone number, is requested.

8. It refers to the closure of the proceedings initially adopted by the AEPD and to the objections of the Portuguese (CNPD) and German (Berlin DPA) authorities, in order to highlight the uncertainty caused by the lack of unity of the criterion for verifying online identity during the management of a right of access.

The GDPR does not lay down, as was the case under the previous legislation, the list of security measures that controllers must adopt; each controller must now carry out its own risk analysis and determine what measures it should take to mitigate them, and this was acknowledged by the AEPD, which considered it reasonable in this case to request additional identification documentation, taking into account the information available, the 'phishing' or social engineering attacks that may occur and unauthorised access to e-mail accounts worldwide.

This is an interpretation based on risk analysis and from good faith and belief of good action, applying the principles of minimisation, privacy by design and by default, on a specific subject (request for identification in the right of access) on which there is no published criterion or guide.

9. With regard to the criteria for graduating the penalty, it states the following:

. Negligence in committing the infringement must be assessed when the conduct deviates from recognised standards and, in this case, when applying for an identity document while managing a right of access, it can now be regarded as 'standard'. In addition, the proactive and improved attitude should be taken into account.

. The volume of data and processing covered by the file is limited to the claim of a single person, or in general annual numbers an average of 55 persons per year, of whom only

one person has requested in the last 4 years.

. The assessment of the number of data subjects should consider the rights exercise requests received since the GDPR is fully implemented, already detailed.

. This is the first time that the requested entity has been the subject of penalty proceedings, complying so far with the obligations laid down in the applicable legislation and with the criteria laid down by the supervisory authorities.

In that regard, it requests that consideration be given to the imposition of a reprimand with particular regard to the nature, minor gravity and short duration of the infringement, its unintentional nature, the measures taken to remedy the damage suffered and the degree of liability demonstrated by the entity.

Page GROUP EUROPE, with its written observations on the opening of the proceedings, submitted the following documents:

- . Copy of the document called "*EU GDPR Data Request Process*". The provisions it contains on the validation of applications for rights and verification of the identity of applicants are set out in Fact 12.
- . Post registration received in the meantime of the technical failure in email from the DPO.
- . Letter of 26 August 2019, sent to the Dutch authority requesting the sending of the missing communication.
- . Letter with the documentation sent in September 2019 to the Dutch Data Protection Authority.

TENTH: On 24 November 2021, a motion for a resolution was issued as follows:

1. That the Director of the AEPD penalises PAGE GROUP EUROPE for an infringement of Article 12 of the GDPR, defined in Article 83 (5) (b) of the GDPR and described as minor for the purposes of limitation in Article 74 (c) of the LOPDGDD, with a fine of 50,000 EUR (fifty thousand euros).

2. That the Director of the AEPD penalises PAGE GROUP EUROPE for an infringement of Article 5 (1) (c) of the GDPR, defined in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (a) of the LOPDGDD, with a fine of 250,000 EUR (two hundred and fifty thousand euros).

The aforementioned draft decision was notified to PAGE GROUP EUROPE on the same date as 24 November 2021. This notification informed this entity that, in accordance with the provisions of Article 85 (2) of the LPACAP, it may, at any time prior to the resolution of the procedure, make the voluntary payment of the proposed penalty, which would result in a reduction of 20 % of the amount of the penalty. With the application of this reduction, the penalty would be set at 240,000 EUR (two hundred and forty thousand euros) and its payment would lead to the closure of the procedure. It was also noted that the effectiveness of this reduction is conditional on the withdrawal or waiver of any administrative action or appeal against the penalty.

ELEVENTH: On 02 December 2021, the requested party paid the penalty in the amount

of 240,000 EUR, making use of the reduction provided for in Article 85 of the LPACAP, which means that the procedure is terminated and any administrative action or appeal against the penalty is waived.

TWELFTH: On 03 December 2021, we received a letter from PAGE GROUP EUROPE dated 02 December 2021, submitting a copy of the proof of the payment made, which it intended to ‘close’ the procedure. In the same letter, the aforementioned entity draws attention to the confidentiality of corporate internal processes.

The actions taken in these proceedings and the documentation contained in the file have shown the following:

PROVEN FACTS

1. Michael Page International is a UK-based company, the parent company of the PageGroup group. It is dedicated to staff selection and operates under various brands, including ‘*Michael Page*’. It has subsidiaries in many European countries, the subsidiary of the Netherlands being Michael Page International — Nederland B.V.

One of the Group’s Spanish subsidiaries, based in Hospitalet de Llobregat, PAGE GROUP EUROPE, S.L., is responsible, through its Legal Compliance Department, for managing requests for the exercise of personal data protection rights that data subjects make to the entities of the PageGroup Group in Europe. The postal address of this Spanish subsidiary is indicated as the contact details for the exercise of these rights in the entity’s privacy policy, both in Spain and in the Dutch version.

2. PageGroup’s websites include a form that allows data subjects to send their CVs to the relevant subsidiary entity.

3. The complainant, a Dutch citizen, opened an account on the website of Michael Page International — Nederland B.V., accessible at the URL “www.michaelpage.nl”, and sent a Curriculum Vitae (CV) for a job offered by this Dutch subsidiary of the PageGroup group in March 2018.

4. By email dated 28 September 2018, sent from the address [REDACTED], the same as recorded in the PageGroup database, the complainant requested access to her personal data, expressly specifying in her request that a copy of her data be sent to her and her interest in knowing the purposes for which the data are processed, the categories of personal data processed, the recipients and the legal basis for each processing operation. That email was sent to the address ‘gdpr@pagegroup.eu’, which corresponds to that indicated for that purpose in the Privacy Policy accessible through the web portal.

In this email, the complainant warns that she receives regular emails from the entity and that this proves that her personal data is available to her.

5. By email dated 02 October 2018, sent from the address ‘gdpr@pagegroup.eu’,

PageGroup replied to the complainant's email of 28 September 2018, stating that in order to comply with the request for access it was necessary to confirm her identity and prove her address. To this end, the complainant is requested to provide two out of three categories of identification documents: (I) passport, national identity card or driving licence showing date of birth; (II) social security or national insurance card; (III) invoice for public services aged less than 3 months. It is also stated that this documentation can be sent to "gdpr@pagegroup.eu" or to the Legal Compliance Department by post to PAGE GROUP EUROPE in Hospitalet de Llobregat.

In addition, this reply informs that if the personal data do not match the recorded ones, further documents will have to be requested and that once the identity has been validated, a copy of the information will be provided within one month.

6. By email dated 20 October 2018, sent to the address "gdpr@pagegroup.eu", the complainant notes that it does not have public utility invoices and that the identification by means of the identity and insurance documents it requires constitutes excessive data processing or an impediment to the exercise of her right. She also points out that the identification process is simplified by considering that she has an account on the entity's website.

7. On 22 October 2018, the Legal Compliance Department of PageGroup sent an email to the complainant, from the address 'gdpr@pagegroup.eu', reiterating the need to verify her identity and insisting on the request for earlier documentation.

8. On 11 November 2018, by email sent to the address 'gdpr@pagegroup.eu', the complainant, after summarising the facts and highlighting her interest in knowing the communications of personal data made to third parties and the specific data shared, reiterated her previous statements on the documentation required to comply with that request, which she considered excessive, and warned about the possibility of lodging a complaint with the Dutch data protection authority.

9. On 12 November 2018, the PageGroup Legal Compliance Department sent an email to the complainant, from the address 'gdpr@pagegroup.eu', informing that they had reviewed her request and requesting that a copy of her identity document be sent by both parties in order to proceed with the request for access.

10. By letter of 14 August 2020, this Agency asked PAGE GROUP EUROPE '*a copy of the reply to the request for access raised by the complainant, since her identity has been proven through the complaint procedure initiated with the supervisory authority of the Netherlands and continued at this Agency*'. Following that request, the aforementioned entity responded to the complainant's request for access and provided the Agency with a copy of the communication dated 27 August 2020, replying to the complainant's request for access, as well as the annex containing the personal data held by PageGroup. The reply to this Agency states that the information was sent by e-mail.

11. In its letter of 10 July 2020, lodged on the same date with the AEPD, PAGE GROUP EUROPE stated that it '*has abolished the procedure whereby two out of three categories of identification documentation were requested. At present, PAGE only requests an identification document and also offers alternatives to data subjects, such as signing by means of an electronic certificate, face-to-face care in any office of PageGroup or any*

other means which the person concerned considers appropriate’.

With that letter, it produced a copy of the new ‘Reply Models’ used to verify the identity of the data subjects. The first of these requests the person concerned to copy the identity card or EIN, passport or driving licence with date of birth, any of them; attention is also drawn to the possibility of using alternative means, should the data subject prefer not to send such documents. The second model refers to such alternative means, such as the presence in a Group office or the sending of a document signed by means of an electronic certificate.

12. PAGE GROUP EUROPE, with its written observations on the opening of the procedure, has provided a copy of the document entitled ‘*EU GDPR Data Request Process*’.

This document indicates that requests to exercise rights are validated if the first name, surname and e-mail match those recorded in their database. In the case of requests for access and portability, it is added that additional information should be requested when there are reasonable doubts about the identity of the applicant, and clarifies that this is the case where there are several persons with the same name or in case of duplication/doubt about the email address.

For the request for additional information, it is envisaged to send an email requesting information already contained in the applicant’s profile registered in his database, and citing as an example the postcode or the last three digits of his or her telephone number.

A template of this request for information is included, requiring one of the two data elements indicated above (postal code and three last digits of the telephone number) and warning that if the data subject does not wish to provide such information, he/she may alternatively apply to a PageGroup office or send a digitally signed document; or communicate whether it has a different means.

In the event that, for any reason, they could receive an identity card or similar documentation from any person concerned, the immediate deletion of that information is required, without using it for validation purposes.

As regards the submission of the document by which the right of access is respected and the corresponding information is provided to the person concerned, the procedure designed by the requested entity provides for it to be sent by email, protected by a password which is sent in a different post.

LEGAL GROUNDS

I

By virtue of the powers conferred on each supervisory authority by Article 58 (2) of the GDPR, and in accordance with Articles 47, 64.2 and 68.1 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to initiate this procedure.

Article 63.2 of the LOPDGDD states that: ‘*The procedures handled by the Spanish Data*

Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures'.

Paragraphs (1) and (2) of Article 58 GDPR list, respectively, the investigatory and corrective powers that the supervisory authority may have for that purpose, by mentioning in point 1 (d) the power to '*notify the controller or processor of an alleged infringement of this Regulation*'; and in paragraph 2. (i), '*to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case*'.

The case under consideration is based on a cross-border complaint to the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) against a group of companies based in the United Kingdom. However, the department responsible for managing access requests for continental Europe is the Legal Compliance Team of the subsidiary of the PAGE GROUP EUROPE Group, based in Spain. This Spanish establishment of PageGroup is the Group's main establishment, within the meaning of the definition in Article 4 (16) GDPR. Thus, in accordance with Article 56 (1) GDPR, the AEPD is competent to act as lead supervisory authority.

The following '*definitions*' set out in Article 4 GDPR are taken into account:

'(16) main establishment:

- (a) *as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.'*

"(21) supervisory authority: the independent public authority which is established by a Member State pursuant to Article 51."

"(22) supervisory authority concerned: the supervisory authority which is concerned by the processing of personal data because:

- A.- *The controller or processor is established on the territory of the Member State of that supervisory authority;*
- B.- *Data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing, or*
- C.- *A complaint has been lodged with that supervisory authority.'*

"(23) cross-border processing:

- (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."*

According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, the personal data protection authorities of the Netherlands, Belgium, Ireland, Poland, Italy, Hungary, Portugal, Cyprus and Austria, as well as the German

regions of North Rhine-Westphalia, Rhineland-Palatinate, Mecklenburg-Western Pomerania, Berlin and Bavaria Private Sector, are acting as '*concerned supervisory authorities*' in the present proceedings.

II

Article 56 (1) of the GDPR, on '*Competence of the lead supervisory authority*', provides:

'1. 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 set out in Article 60'.

*Article 60 governs '*Cooperation between the lead supervisory authority and the other supervisory authorities concerned*':*

- 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.*
- 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.*
- (...)*
- 12. The lead supervisory authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.'*

With regard to the matters governed by these provisions, account is taken of recitals 124, 125, 126 and 130 of the GDPR, in particular the following:

(124) ‘... that authority (the lead authority) should cooperate with the other authorities concerned...’.

(125) ‘as lead authority, the supervisory authority should closely involve and coordinate the supervisory authorities concerned in the decision-making process’.

(126) ‘the decision should be agreed jointly by the lead supervisory authority and the supervisory authorities concerned...’.

(130) ‘Where the supervisory authority with which the complaint has been lodged is not the lead supervisory authority, the lead supervisory authority should closely cooperate with the supervisory authority with which the complaint has been lodged in accordance with the provisions on cooperation and consistency laid down in this Regulation. In such cases, the lead supervisory authority should, when taking measures intended to produce legal effects, including the imposition of administrative fines, take utmost account of the view of the supervisory authority with which the complaint has been lodged and which should remain competent to carry out any investigation on the territory of its own Member State in liaison with the competent supervisory authority’.

In accordance with Article 4 (24) GDPR, ‘relevant and reasoned objection’ means the following:

‘an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union’

In accordance with the above rules, in the present case, concerning a complaint lodged with the supervisory authority of a Member State (the Netherlands), in relation to processing operations in the context of the activities of an establishment of a controller which affect or are likely to substantially affect data subjects in more than one Member State (cross-border data processing), the lead supervisory authority, in this case the Spanish Data Protection Agency, is required to cooperate with the other authorities concerned.

The Spanish Data Protection Agency, in application of the powers conferred on it by the GDPR, is competent to adopt decisions designed to produce legal effects, whether the imposition of measures ensuring compliance with the rules or the imposition of administrative fines. However, it is obliged to closely involve and coordinate the supervisory authorities concerned in the decision-making process and to take their views into account to the greatest extent. It also provides that the binding decision to be taken is to be agreed jointly.

Article 60 GDPR regulates this cooperation between the lead supervisory authority and the other supervisory authorities concerned. Paragraph 3 of that article expressly provides that the lead supervisory authority shall, without delay, forward to the other supervisory authorities concerned a draft decision for their opinion and shall take due account of their views, in accordance with the procedure laid down in paragraphs 4 et seq. The supervisory authorities concerned have a period of four weeks to raise reasoned objections to the draft decision, it being understood that there is agreement on the draft decision if no authority objects within the period indicated, in which case all of them are bound by the draft decision.

In another case, i.e. if any of the authorities concerned raises a relevant and reasoned

objection to the draft decision, the lead supervisory authority may follow the objection by submitting to the opinion of the other supervisory authorities concerned a revised draft decision, which shall be submitted to the procedure referred to in paragraph 4 within two weeks. If no further action is taken in the objection or if the objection is deemed not to be relevant, the lead supervisory authority should refer the matter to the consistency mechanism provided for in Article 63 GDPR.

In the present case, the AEPD initially considered that there was no indication of an infringement and that it was not necessary to call for the adoption of measures additional to those implemented by PAGE GROUP EUROPE, with the result that, on 10 November 2020, a draft decision was issued, whereby the other supervisory authorities concerned were required to close the complaint (Draft Decision).

At the end of the prescribed period, the Data Protection Authorities of Portugal (CNPD) and Berlin (The Berlin Commissioner for Data Protection and Freedom of Information — Berlin DPA) raised objections to the draft decision, as set out in the background to this agreement.

Taking into account the reasons set out in the objections raised, and in accordance with Article 60(1) of the GDPR, as transcribed above, which obliges the lead supervisory authority to cooperate with the other authorities, in an effort to reach consensus, the procedure provided for in Article 60 (5) was followed instead of resorting to the consistency mechanism provided for in Article 63 of the GDPR.

Although, as the requested entity points out in its submissions, it initially considered that there were no indications of an infringement, after analysing the observations or objections raised by the supervisory authorities concerned, certain circumstances were revealed which had not been sufficiently assessed in the draft decision, which will be set out in the following legal grounds.

It was therefore appropriate to draw up a revised draft decision providing for the opening of penalty proceedings against PAGE GROUP EUROPE.

This is in line with the cooperation procedure regulated in Article 60 GDPR; it also takes into account Article 58 (4) of the same Regulation, according to which the exercise of the powers conferred on the supervisory authority must respect the procedural safeguards laid down in Union and Member State law.

Spanish procedural rules, in particular Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), provide that proceedings of a sanctioning nature shall always be initiated *ex officio* by agreement of the competent body, which must contain, among other information, the identification of the person or persons presumed to be responsible, the facts giving rise to the initiation of the proceedings, their possible classification and the penalties that may apply.

The adoption of the draft agreement initiating penalty proceedings is provided for in Article 64 (2) (third subparagraph) and (3) of the LOPDGDD, with the obligation to give formal notice to the person concerned. That notification interrupts the limitation period for the infringement.

The revised draft decision drawn up by the AEPD, in the form of a draft initiating penalty proceedings, was submitted for consideration to the authorities concerned, so that they could raise any objections they considered relevant or agree to them. To that end, it was sent via the IMI system to those authorities, informing them that, if no objections were raised within two weeks of the consultation, the necessary agreement to initiate penalty proceedings would be adopted. None of the supervisory authorities concerned raised any objections and it was therefore understood that there was agreement on the draft in question.

Consequently, on 29 June 2021, the AEPD decided to initiate the present penalty proceedings, in accordance with the arguments and allegations contained in the draft revised decision.

Furthermore, Article 64 (4) of the LOPDGDD provides that the processing times laid down in this Article are automatically suspended when information, consultation, request for assistance or mandatory ruling from a body, office or agency of the European Union or from one or more supervisory authorities of the Member States must be obtained in accordance with the GDPR, for the time between the request and the notification of the decision to the Spanish Data Protection Agency.

III

In accordance with Article 55 of the GDPR, the Spanish Data Protection Agency is responsible for carrying out the tasks assigned to it in Article 57 of the GDPR, including enforcing the Regulation and raising awareness among controllers and processors of their obligations, as well as dealing with complaints lodged by a data subject and investigating the reasons for such complaints.

Correspondingly, Article 31 GDPR establishes an obligation for controllers and processors to cooperate with the supervisory authority upon request in the performance of their tasks. In the event that they have appointed a data protection officer, Article 39 of the GDPR entrusts the latter with the task of cooperating with that authority.

Similarly, Article 65 (4) of the LOPDGDD provides for a mechanism prior to the admissibility of complaints lodged with the Spanish Data Protection Agency, which consists of sending them to the data protection officers designated by the controllers or processors for the purposes laid down in Article 37 of that law, or to the latter where they have not been designated, so that they can analyse those complaints and respond to them within one month.

In accordance with these rules, prior to the admissibility of the complaint giving rise to the present proceedings, it was sent to the responsible entity for analysis, a reply to this Agency within one month and proof that it had provided the complainant with the appropriate reply in the event of the exercise of the rights provided for in Articles 15 to 22 of the GDPR.

The result of that transfer was not satisfactory, given the procedure followed by the draft decision and the objections raised in that regard, so that it was considered appropriate to continue to take steps to clarify the possible responsibilities identified. Consequently,

on 11 December 2020, for the purposes laid down in Article 64 (2) of the LOPDGDD, the Spanish Data Protection Agency declared admissible the complaint communicated by the Dutch Data Protection Authority (Autoreit Persoonsgegevens -AP) concerning alleged infringements related to the exercise of the rights granted to the holders of personal data. That decision to grant leave to proceed led to the opening of these penalty proceedings.

As regards exclusively a complaint for failure to comply with a request to exercise the rights set out in Articles 15 to 22 of the GDPR, the procedure laid down in Article 64 (1) of the LOPDGDD is followed, according to which:

'When the procedure is exclusively referred to the lack of response to a request to exercise the rights established in articles 15 to 22 of Regulation (EU) 2016/679, it shall be initiated by a resolution to admit for processing, which shall be adopted in accordance with the provisions of Article 65 of this organic law'.

Conversely, where the procedure does not relate exclusively to a request for the exercise of rights, it is necessary to define administrative responsibilities in the context of penalty proceedings, and it is the exclusive competence of the Agency to assess whether there are administrative responsibilities which must be determined in such a procedure and, consequently, to decide on the initiation of such proceedings.

In this case, there are elements justifying the exercise of the sanctioning activity, considering that the procedure provided for in Article 64 (1) of the aforementioned LOPDGDD would not adequately restore the guarantees and rights of the persons concerned.

The origin of the proceedings is determined by a complaint lodged by a specific data subject, which concerns the lack of attention to the right of access exercised by the complainant before the requested body. It could therefore be thought that this is the procedure governed by Article 64 (1) of the LOPDGDD.

However, this claim by an individual has revealed a general action by the controller, and this particular case reflects a common pattern or policy applied to all those affected who are in the same case as the complainant. Where an action which is deemed to be incorrect results from a general policy adopted by the controller, so that it is not a one-off error in a case, the infringement does not lie exclusively in the case under examination but in that general action taken by the controller.

The contrary would be inconsistent with the aim and intention of the Community legislature, which is expressly stated in the GDPR when it states that it is for the supervisory authorities to enforce the rule.

Consequently, this procedure analyses the impact of the general action taken by PAGE GROUP EUROPE on the management and resolution of requests for the exercise of access and portability rights made to it by data subjects, the processing of which is limited and conditional on the documentation requirements generally imposed by that body in order to verify the identity of the applicant, which do not comply with the legislation governing these rights of data subjects, as will be explained below.

In view of the shortcomings noted in the procedure devised by the requested body with

regard to the data protection rules, it appears that those deficiencies are of general application, so that all the data subjects who made the abovementioned requests, and not only the complainant, are affected.

This is concluded in the light of the information and statements that the requested entity itself has provided to this Agency, in which it acknowledges that the process of taking care of rights was in line with the design carried out by the Agency and sets out the reasons that led it to implement a strict identity verification process, based, among other things, on the nature of the human resources services it provides, the large number of candidates and the fact that the exercise of rights is very common, as well as attacks by phishing or social engineering. It defends its system on the ground that it is due to an excessive dirt on the part of the entity.

It expressly stated that it '*abolished the procedure whereby two out of three categories of identification documentation were requested*'.

The information provided by the requested entity is also consistent with the action taken in relation to the complainant's specific request for access.

We therefore do not understand that PAGE GROUP EUROPE, in its submissions to the opening of the procedure, claims that it made an error in explaining the aforementioned rights management process and that it modified its previous approach in order to set out circumstances that do not reflect reality. The fact is that, as demonstrated in the proceedings, the identity verification scheme designed by the respondent applied to all cases of exercise of rights of access and portability, in general, and not only to cases where there were doubts as to the identity of the applicant, as stated in its submissions; that verification required the production by the data subject of several identification documents and not a single document, as appears to be conveyed in the repeated submissions.

Moreover, PAGE GROUP EUROPE states in its written pleadings that it has followed the recommendations of the authorities, however, it does not mention which recommendations would justify the following procedure.

Throughout the text of its written pleadings it refers only to the "*Guide for Citizens*" drawn up by the AEPD and the instructions containing the forms for exercising the rights that the AEPD makes available to citizens via its website. In both cases, as the requested entity rightly points out, citizens are informed of the possibility that the controllers may request photocopy of the ID card or equivalent document, but it should be noted that this should be the case where the controller has doubts about the identity of the applicant and also that the electronic signature may be used instead of the identification document.

The content of those documents does not contradict the criteria set out in this act. It should be noted that the specific objective covered by these guides is to provide guidance on best practices in more general cases, so that they do not cover all specific scenarios that may arise and this implies that the guidance contained therein should be supplemented as appropriate.

Finally, it should be pointed out at this stage that the conclusions set out below are obtained by applying the rules laid down by the GDPR and the LOPDGDD, without

considering repealed legislation, such as Royal Decree 1720/2007, or cultural aspects or historical issues inherited from local regulations, to which the requested entity refers in its written pleadings.

IV

The rights of individuals with regard to the protection of personal data are regulated in Articles 15-22 GDPR and 13-18 LOPDGDD. It provides for the rights of access, rectification, erasure, objection, right to restriction of processing and right to portability.

The formal aspects of the exercise of these rights are set out in Articles 12 GDPR and 12 LOPDGDD.

Article 12 ‘transparent information, communication and modalities for the exercise of the rights of the data subject’ of the GDPR provides:

- ‘1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
2. The controller shall facilitate the exercise of data subject 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.
3. 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. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
4. 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.
5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:
 - (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
 - (b) refuse to act on the request.
 The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.
6. 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.
7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly

legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.'

Article 12 (2) and (4) of the LOPDGDD, 'General provisions on the exercise of rights', adds the following:

'2. The controller shall be obliged to inform the data subject about the means available to exercise their rights. Such means shall be easily accessible by the data subject. The exercise of the right may not be denied on the sole ground that the data subject chooses a different means'.

'4. The evidence of compliance with the duty to respond to the request for the exercise of rights submitted by the data subject shall be the responsibility of the controller'.

Account is also taken of recitals 59 et seq. of the GDPR.

In accordance with these rules, the controller must devise formulas and mechanisms to facilitate the exercise by the data subject of his or her rights, which shall be free of charge (without prejudice to Articles 12.5 and 15.3 GDPR); is obliged to respond to requests made within one month at the latest, unless it can prove that it is not in a position to identify the data subject; and to state its reasons in case of failure to comply with the request.

It follows from the foregoing that the request for the exercise of rights made by the data subject must in any event be answered, the controller being required to prove compliance with that duty.

This obligation to act does not apply where the controller can demonstrate that it is not in a position to identify the data subject (in the cases referred to in Article 11 (2) GDPR). In cases other than that provided for in this Article, where the controller has reasonable doubts as to the identity of the applicant, the controller may request additional information necessary to confirm that identity.

In that regard, recital 64 of the GDPR is worded as follows:

'(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests'.

As regards the right of access, the GDPR stipulates in its Article 15 that:

"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 recipients to whom the personal data have been or will be disclosed, in particular recipients in third parties or international organisations;*
- (D) where possible, the envisaged period of storage of personal data or, if that is 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 have not been obtained from the data subject, any available information as to their origin;
- (h) the existence of automated decision-making, including profiling, as referred to in Article 22 (1) and (4), and, at least in such cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject."

2. Where personal data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of appropriate safeguards pursuant to Article 46 concerning 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.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.'

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.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others'.

Like the other rights of the data subject, the right of access is an extremely personal right. It allows citizens to obtain information about the processing of their personal data, the possibility to obtain a copy of their personal data which are being processed, as well as the information listed in the aforementioned article.

In the present case, the complainant, a Dutch citizen, opened an account in the Dutch version of the website of Michael Page International, accessible at the URL 'www.michaelpage.nl', and sent a Curriculum Vitae (CV) for a job offered by the Dutch subsidiary of the PageGroup group by that channel in March 2018.

Subsequently, on 28 September 2018, she exercised the right of access to her personal data by email sent to the address 'gdpr@pagegroup.eu', which corresponds to that indicated for that purpose in the privacy policy of the web portal, expressly stating in this request her interest in knowing the data processed, the purposes for which they are processed, the recipients and the shared data, as well as the legal basis for each processing operation (this request is in line with the content of the right of access provided for in Article 15 of the GDPR), that, as explained above, not only does it involve informing the applicant of the personal data or categories of data processed, so that the exceptional nature attributed to it by the requested entity is not understood when it claims that such requests for access are not frequent since it is the data subjects themselves who directly provide their personal data and have the information available to them in their personal area).

The request made by the complainant is sent from the same e-mail address of the complainant as registered in the PageGroup database, which, according to the complainant, was being used by the Dutch subsidiary of the Group to send her work offers and commercial communications.

In response to this request, on two occasions, the requested entity sent an email to the complainant requiring her to provide documentation proving her identity, establishing this requirement as a condition for complying with the right exercised. In particular, it required the production of two out of three categories of identification documents: (I) passport, national identity card or driving licence showing date of birth; (II) social security or national insurance card; (III) invoice for public services aged less than 3 months.

Also on two occasions, by e-mails dated 20 October and 11 November 2018, the complainant warned that the required identification constitutes excessive data processing or an impediment to the exercise of her right and expressly pointed out that the identification process is simplified by considering that she has an account on the entity's website.

It would not be until 12 November 2018, after the complainant communicated her intention to lodge a complaint with the Dutch data protection authority, when PAGE GROUP EUROPE amended its initial requirements, but maintained the request for the complainant's identity card (copy by both sides) in order to proceed with the request for access.

On the question of verification of the identity of applicants for rights, the rules set out above are clear by stating that this verification process must be limited to specific cases

in which the controller has '*reasonable*' doubts as to the identity of the natural person making the application.

Article 12 (6) GDPR refers to all requests for rights and allows for the possibility to require, in such cases, "*additional information*" necessary to confirm the identity of the data subject. In particular, with regard to access requests in the context of online services, Recital 64 of the same Regulation refers to the possibility for the controller to use all '*reasonable measures*' to verify the identity of data subjects.

The rules governing the exercise of rights do not, therefore, establish the need to provide any specific identification document in order for them to be met, nor do they even require such identity verification to be carried out on the basis of documentation. They refer to the possibility of obtaining '*additional information*' and the use of '*reasonable measures*', whereby it is for the controller to determine what information and measures are reasonable in each case, taking into account the circumstances of the case and always using means that are least intrusive to the privacy of applicants. All of this, subject to the condition that it is a case in which there is '*reasonable doubt*' as to the identity of the applicant.

Page GROUP EUROPE has not justified the existence of such reasonable doubts regarding the complainant's identity. On the contrary, that entity's actions are in accordance with the rights management procedure which it has itself designed, in its capacity as controller, which required the documentation referred to above in all cases, without first analysing whether or not such reasonable doubts were raised.

Nor does the procedure designed by the requested entity provide for the possibility of verifying the identity of the applicant by means of other information or measures other than the provision of supporting documents.

In this case, the complainant was registered in the information systems of the responsible entity, which had extensive information about it; and that the request for access to personal data was made from the same email address of the complainant as was already in the database of the complainant.

It is therefore not understood that this case has been treated as one of those cases where there are doubts as to the identity of the applicant (this is only explained by considering that all the cases of access and portability were thus considered by the respondent); and that, without any other basic approach, PAGE GROUP EUROPE required the provision of several identification documents (those identified), when it had less intrusive means to ensure that the information would be sent to the data subject, such as having checked some of the data already available.

Page GROUP EUROPE was aware of the complainant's contact details, so that the request received from the email address that the entity had registered in its systems and the sending of the requested information with access to that address provided sufficient guarantees, in the opinion of the Agency, to have complied with the request received. Moreover, it has not been established that there was any circumstance that led the requested entity to think of an identity theft or a computer attack.

The strict requirements imposed on the complainant to comply with her request for

access led to the fact that this request was left unanswered, despite the two warnings issued by the complainant herself regarding the excessive requests for documentation sent to her; they determined that the complainant chose to go to the data protection authority of the Netherlands instead of continuing the processing of her application, as she had warned in her email of 11 November 2018.

Consequently, PAGE GROUP EUROPE is responsible for ensuring that the deadline set for responding to the complainant's request elapses without a proper reply, providing it with the requested information.

The right of access was finally granted on 27 August 2020, during the processing of the complaint carried out by this Agency as the lead supervisory authority, following an express request from this Agency dated 14 August 2020. In this regard, it should be pointed out that the response to the request for access cannot be expressed in the context of a mere administrative procedure, such as the forwarding of the complaint to the requested party pursuant to Article 64 (3) of the LOPDGDD.

Consequently, in accordance with the evidence set out above, the aforementioned facts constitute an infringement of Article 12 (2) and (3) of the GDPR, as a result of the failure to take account of the right of access exercised by the complainant, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of that Regulation.

V

In response to the complainant's request for access of 28 September 2018, the responsible entity initially required the complainant to provide two out of three categories of identification documentation: passport, national identity card or driving licence showing date of birth; social security or national insurance card; or invoice for public services aged less than 3 months.

As set out in the previous legal ground, this action by the requested entity responds to the rights management procedure which it has itself designed, as the controller, which required the documentation referred to above in all cases and without considering the possibility of verifying the identity of the applicant by means of information other than the documents referred to above.

The complainant considered that there was no reason to require such identifying information as necessary for the attention of the law, considering that it was not required to open an account on the web portal or to submit its CV. According to the complainant, the authenticated access to the account, which was still active at the time when the request was made to the responsible entity, should be sufficient to understand the exercise of the right and prove her identity in a system such as that used by the controller, based on the use of a private account.

The arguments put forward by the supervisory authorities CNPD and Berlin DPA, mentioned in the Fourth Fact, which have already pointed out that the procedure put in place for the attention of rights do not discriminate against cases where there are doubts as to the identity of the applicant who do not; whereas this procedure does not protect

the data of applicants and increases the risks for those concerned; whereas this documentation is not required from data subjects to open an account or send a CV; additional information should only be requested if there are doubts as to the identity of the data subject, requesting information necessary and appropriate for such verification, on the basis of the applicant's available data.

Both supervisory authorities advocate a less intrusive way of verifying the identity of the applicant, other than the verification of the identity card (e.g. electronic identification or sending the application via the user account together with an additional authentication factor sent via another channel); and agree with the complainant that access to the private account should be understood as sufficient.

They also serve, by coincidence, the arguments set out in the previous legal basis, concerning the possibility of requesting additional information necessary to confirm the identity of the data subject only where the controller has reasonable doubts as to the identity of the applicant for the right (Article 12 (6) GDPR).

PAGE GROUP EUROPE has acknowledged that the identification documentation required from the complainant to verify her identity was required in all cases of exercising rights (at least for requests for access or portability), following the procedure designed by the complainant itself. As stated, it sought to ensure that candidates' personal data were not transferred to third parties who could have access to the credentials of persons registered in their systems for the purpose of deleting their identity and making the application on their behalf, through phishing or social engineering attacks.

In order to assess these facts, account must also be taken of Articles 25 and 32 of the GDPR, which provide that:

'Article 25. Data protection by design and by default.'

1. 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.

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article'.

'Article 32. Security of processing.'

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) *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
 - (d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the 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.*
- (...)

In this case, the system designed by PAGE GROUP EUROPE lays down requirements for the attention of data subjects' rights which go beyond what is provided for in the legislation governing these rights; they do not meet any of the criteria and factors referred to in Article 25 (1) of the GDPR, such as the context, the risks or the purpose of the processing.

Moreover, it is clear that using two of the three documents required by PAGE GROUP EUROPE to verify the identity of the applicants for rights does not guarantee that only personal data that are necessary for this specific purpose are processed.

Against this, the respondent's arguments that the use of those documents is limited to verifying that the applicant's name corresponds to the data available (if that was the case, it is not understood that the date of birth was expressly required), that they are deleted immediately after that check (a fact which has not been proven or was initially stated) and that their access is made solely by the Department of Legal Compliance and, ultimately, the DPO, are insufficient.

The excess, in this case, is apparent simply from the collection of the documents requested by the respondent.

For the same reasons, it is considered that the processing of personal data contained in the identification documents that PAGE GROUP EUROPE requested, in general, from persons making a request to exercise access and portability rights, which were not necessary for the management of that request, increase the risks for those concerned and does not guarantee a level of security appropriate to the risk.

As a result, the provision by any data subject of the documentation required by PAGE GROUP EUROPE in order to verify his or her identity, in the context of a request to exercise the right of access or portability, results, in the circumstances indicated, in the processing of inappropriate, irrelevant and not necessary personal data for this specific purpose of the processing, contrary to the data protection principles, in particular the principle of '*data minimisation*' laid down in Article 5 (1) (c) GDPR:

'Article 5 Principles relating to processing of personal data'

1. Personal data shall be:

- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').*

As regards the scope of that principle, recital 39 of the GDPR states that '*personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*'.

There is no need to insist on the fact that in the cases analysed there is no need to collect identification documentation from persons applying for a right, as there are other reliable, less intrusive means of identification; the collection of several identity documents is even less necessary.

The respondent required the production of two out of three documents (passport, national identity card or driving licence, showing the date of birth; social security or national insurance card; or invoice for public services aged less than 3 months), and it would not be until the complainant's repeated protest that PAGE GROUP EUROPE considered the request for documentation excessive and corrected to request a copy of a single identification document on both sides. Rectification that does not resolve non-compliance with the data minimisation principle.

The petitioner also considers that the absence of further processing of the data contained in the identification documents, their limited and exclusive use by the legal compliance team makes its action compatible with the principle of minimisation, as it is necessary, proportionate and appropriate to protect the rights of the data subject, thus complying with recital 156 of the GDPR, according to which '*The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles*'.

However, this recital refers to processing for archiving purposes in the public interest and cannot be referred to in the present case.

Consequently, the above-mentioned facts, in relation to the data processing involved in the rights management procedure followed by PAGE GROUP EUROPE for the verification of the identity of the data subjects, constitute an infringement of Article 5 (1) (c) of the GDPR, which gives rise to the application of the corrective powers conferred on the Spanish Data Protection Agency by Article 58 of that Regulation.

VI

In the event of an infringement of the provisions of the GDPR, among the corrective powers available to the Spanish Data Protection Agency as the supervisory authority, Article 58 (2) of the GDPR provides for the following:

- '2 each supervisory authority shall have all of the following corrective powers:
(...)
(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;'*
- (...)*
- (d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;*
- (...)*

(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.'

According to Article 83 (2) GDPR, the measure provided for in point (d) above is compatible with the penalty consisting of an administrative fine.

VII

The facts set out above do not comply with the provisions of Articles 12 and 5.1 (c) of the GDPR, with the scope set out in the preceding legal bases, which entails the commission of infringements set out in Article 83 (5) (b) and (5) (a) of the GDPR, which, under the heading '*General conditions for the imposition of administrative fines*', provides as follows:

'5. 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.*
- (b) the data subjects' rights within pursuant to Articles 12 to 22'.*

In this regard, Article 74 of the LOPDGDD considers that infringements of a purely formal nature of the articles referred to in Article 83 (5) of the GDPR and, in particular, '*(c) failing to attend to the requirements to exercise any of the rights established by Articles 15 to 22 of Regulation (EU) 2016/679, unless this results from the implementation of Article 72 (1) (k) of this Organic Law*', is regarded as a '*minor*' infringement for the purposes of limitation period.

For its part, Article 72 (1) (a) of the LOPDGDD considers, for the purposes of limitation period, as '*very serious*':

'1. In accordance with article 83.5 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered very serious infringements and its limitation period shall be three years:

- (a) The processing of personal data which infringes the principles and guarantees provided for in article 5 of Regulation (EU) 2016/679.'*

In order to determine the administrative fine to be imposed, it is necessary to comply with the provisions of Articles 83.1 and 83.2 of the GDPR, which state:

'1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). 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.'

Article 76 of the LOPDGDD, entitled '*Penalties and corrective measures*', provides:

- '1. Penalties provided by sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679 shall apply considering their degree and the criteria established in section 2 of the aforementioned article.
- 2. Pursuant to the provisions of article 83.2.k) of Regulation (EU) 2016/679, the following criteria may also be considered:

- (a) The ongoing nature of the relevant infringement.
- (b) The existence of a link between the perpetrator's activities and their processing of personal data.
- (c) Any profits obtained as a consequence of the relevant infringement.
- (d) The possibility that the perpetrator's activities have induced them to commit the relevant infringement.
- (e) The existence of a merger by acquisition subsequent to the infringement, which may not be attributed to the acquiring company.
- (f) Whether the rights of minors have been affected.
- (g) The existence of a Data Protection Officer, in those cases when their appointment is not compulsory'.
- (h) Voluntary submission by the data processor or the data controller to alternative dispute resolution methods, in those cases in which disputes arise between the data processor or the data controller and any other stakeholder.'

In this case, having regard to the gravity of the infringements found, it is appropriate to impose a fine and, where appropriate, to adopt measures. The request made by PAGE GROUP EUROPE for the imposition of other corrective powers, such as the reprimand, which is provided for natural persons and where the penalty constitutes a disproportionate burden, cannot be accepted (recital 148 GDPR). In this regard, the Agency does not agree that the infringements found are of minor gravity, taking into account the effects they have had on the exercise of the rights granted to data subjects; nor the short duration claimed by the respondent, given that the irregular process of managing those rights has been imposed since the time when the GDPR became applicable.

In accordance with the above provisions, for the purpose of determining the amount of the penalties to be imposed in the present case, it is considered that the fines should be graduated according to the following criteria:

1. Infringement of Article 12 of the GDPR, defined in Article 83 (5) (b) and classified as minor for the purposes of limitation in Article 74 (c) of the LOPDGDD:

The following criteria for graduation are considered to be aggravating factors:

- . Article 83 (2) (a) GDPR: '*(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.*
- . The nature of the infringement, in that the lack of attention to the right of access, due to its content, affects the complainant's ability to exercise genuine control over her personal data.
- . The nature of the harm caused to the data subject, who was deprived of one of her basic rights with regard to the protection of personal data, despite the communications sent by the data subject, insisting on his or her interest.
- . Article 83 (2) (d) GDPR: "*(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.*"

The entity charged does not have adequate procedures in place to act on the collection and processing of personal data, as regards the management of requests for the exercise of rights, so that the infringement is not the result of an anomaly in the operation of those procedures but of a defect in the personal data management system designed by the controller. That procedure was adopted by the defendant on its own initiative laying down requirements going beyond the applicable legislative provisions.

- . Article 76 (2) (b) of the LOPDGDD: "*(b) The existence of a link between the perpetrator's activities and their processing of personal data.*"

The fact that the infringer's activity is closely linked to the processing of personal data, taking into account the activity it carries out in the human resources sector and the level of establishment of the entity (Sixth Fact contains some details on this implementation).

- . Article 83 (2) (k) GDPR: "*(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.*"

The status of large enterprise and turnover of PageGroup and PAGE GROUP EUROPE (see Sixth Fact for some details).

The following circumstances are also considered to be mitigating:

- . Article 83 (2) (f) GDPR: "*(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 right of access exercised by the complainant was ultimately granted by the requested entity, although the intervention of the supervisory authorities was required.

PAGE GROUP EUROPE, in its written pleadings, did not make any statement regarding the criteria and factors assessed for grading this infringement.

In view of the factors set out above, the assessment of the fine for infringement of Article 12 of the GDPR is 50,000 EUR (fifty thousand euros).

2. Infringement for failure to comply with the provisions of Article 5 (1) (c) of the GDPR, defined in Article 83 (5) (a) and classified as very serious for the purposes of limitation in Article 72 (1) (a) of the LOPDGDD:

The following criteria for graduation are considered to be aggravating factors:

- . Article 83 (2) (a) GDPR: “*(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*”
- . The nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing operations concerned. The infringement concerns fundamental aspects of data protection and results in the processing of identification documents of data subjects, in accordance with the rights management procedure that implemented the requested person at the time when the GDPR became applicable, which has not been rectified until the opening of the procedure.
- . The number of data subjects affected: the infringement concerns all data subjects who have exercised the right of access or portability, although it is necessary to consider the significance that the infringing conduct may have had on all of the entity's customers, many of them considering the level of international implementation of the infringement.
- . The nature of the damage caused to the data subjects, who have seen their rights limited and the risk to their privacy increased.
- . Article 83 (2) (b) GDPR: ‘*(b) the intentional or negligent character of the infringement*’.

The negligence found to have been committed in committing the infringement.

In that regard, the argument put forward by PAGE GROUP EUROPE that negligence must be assessed when the conduct deviates from recognised standards cannot be accepted. If an action deviates from the standard, it cannot be said that it meets the standards.

Furthermore, in relation to the complainant's request for access, despite the complainant's allegations that the documentation requested from it was excessive, it continued to request that documentation and did not comply with the right until the intervention of the supervisory authorities.

- . Article 83 (2) (d) GDPR: '(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.'

The entity charged does not have adequate procedures in place for the collection and processing of personal data, so that the infringement is not the result of an anomaly in the operation of those procedures but of a defect in the personal data management system designed by the controller.

- . Article 76 (2) (a) of the LOPDGDD: '(a) the ongoing nature of the relevant infringement'.

The rights management procedure put in place by the respondent applied to all requests to exercise access and portability rights that customers have made since the GDPR became applicable. This is a number of actions following the action designed by PAGE GROUP EUROPE, which infringe the same provision.

- . Article 76 (2) (b) of the LOPDGDD: '(b) the existence of a link between the perpetrator's activities and their processing of personal data'.

The fact that the activity of the infringer is closely linked to the processing of personal data, taking into account the reasons already expressed when setting out the factors used to determine the scale of the previous infringement.

- . Article 83 (2) (k) GDPR: '(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, through the infringement.'

- . The volume of data and processing that is the subject of the file, taking into account the level of information requested from persons accessing its services.
- . The status of large enterprise and turnover of PageGroup and PAGE GROUP EUROPE.

The following circumstances are also considered to be mitigating:

- . Article 83 (2) (c) GDPR: 'Any action taken by the controller or processor to mitigate the damage suffered by data subjects'.
- . Article 83 (2) (f) GDPR: 'The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement'.

PAGE GROUP EUROPE has designed a new rights management procedure to remedy the concerns that have led to infringements being committed. However, it should be borne in mind that this remedy did not take place until after the procedure had been opened.

In view of the factors set out above, the assessment reached by the fine for infringement of Article 5 (1) (c) of the GDPR is 250,000 EUR (two hundred and fifty thousand euros).

None of the graduation factors considered is mitigated by the fact that the requested entity has not previously been the subject of penalty proceedings, a fact which has been invoked by the requested entity to be considered a mitigating factor.

In this regard, the judgment of the NA of 05 May 2021, rec. 1437/2020, states that '*It also considers that the failure to commit an earlier infringement should be regarded as as mitigating. Article 83 (2) of the GDPR provides that account must be taken of, inter alia, '(e) any previous infringement committed by the controller or processor' for the purposes of imposing the administrative fine. This is an aggravating circumstance, the fact that the budget for its application is not met means that it cannot be taken into consideration, but does not imply or permit, as the applicant claims, its application as an attenuating factor.'*

PAGE GROUP EUROPE also refers in its submissions to two actions taken by the data protection authority of the Netherlands for illegal processing of identity documents in which the companies concerned were not penalised, although, according to the requested entity itself, these are actions prior to the entry into force of the GDPR. Furthermore, the details which determined those agreements are not provided.

VIII

Infringements may result in the controller being required to *take appropriate measures to bring its action in line with the rules referred to in this act, in accordance with the aforementioned Article 58 (2) (d) GDPR, according to which each supervisory authority may 'order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period'*. Failure to comply with this body's requirements may be regarded as a serious administrative offence because it '*does not cooperate with the supervisory authority*' in response to such requests, and such conduct may be assessed when administrative proceedings are initiated with a pecuniary fine.

In such a case, in the decision to be adopted, the Agency may require the entity responsible to comply, within a period to be determined, with the rules on the protection of personal data, the processing operations it carries out and the mechanisms and procedures it follows to meet requests for the exercise of rights made to it by data subjects, to the extent set out in the legal bases of this Agreement.

Likewise, the measures which may be taken in the decision terminating the proceedings, in relation to processing activities and the exercise of rights, shall apply in all the countries of the European Union in which PageGroup operates.

In this case, following the complainant's complaint, which considered the documentation required to prove her identity to be excessive when exercising the right of access, the responsible entity corrected and requested only a copy of the identification document on both sides.

In addition, PAGE GROUP EUROPE, when the complaint was sent, stated that it '*has abolished the procedure whereby two out of three categories of identification documentation were requested. At present, PAGE only requests an identification document and also offers alternatives to interested parties, such as signing by means of*

an electronic certificate, face-to-face care in any office of PageGroup or any other means which the person concerned considers appropriate'.

In that regard, it provides a copy of the '*Reply Models*' used at that date to verify the identity of the data subjects. The first of these requests the data subject to copy the identity card or EIN, passport or driving licence with date of birth, any of them; attention is also drawn to the possibility of using alternative means, should the data subject prefer not to send such documents. The second model refers to such alternative means, such as the presence in a Group office or the sending of a document signed by means of an electronic certificate.

These measures represent an improvement compared to the procedure initially followed, the one applied to the complainant, which required two identification documents and not only one, but did not fully correct the concerns raised in this act.

However, in its written pleadings to the opening of the procedure, the aforementioned entity provided the document entitled '*EU GDPR Data Request Process*', which sets out the way in which it is currently dealing with requests for the exercise of rights. This new process abandons the practice of requiring identification documents for the purpose of dealing with access requests, which validate only by means of the applicant's first name, surname and e-mail and his/her match with those registered in his/her information system.

It also sets out the cases in which additional information should be required, where there are reasonable doubts as to the identity of the applicant, in cases where there are several persons with the same name or in case of duplication/doubt about the e-mail address. In such cases, it intends to send an email to the data subject requesting information already contained in the applicant's profile registered in his or her database, and cites as an example the postcode or the last three digits of his or her telephone number.

In addition, it provides for alternative means to enable the person concerned to prove his/her identity, in the event that he/she is unwilling to provide the additional information (to be presented to a PageGroup office or to send a document bearing a digital signature; or communicate whether it has a different means); it has planned not to process any identity document it might receive, by deleting it immediately.

It is considered that these new measures implemented by PAGE GROUP EUROPE comply with the criteria assessed in these actions, in relation to the procedures for managing applications for the exercise of rights and the means of validating the identity of applicants, and it is not appropriate to impose additional measures.

IX

Article 85 of Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), *entitled 'Termination in penalty proceedings'*, provides:

- "1. Once penalty proceedings have been initiated, if the offender recognises his liability, the proceedings may be resolved by the imposition of the appropriate penalty.*
- 2. Where the penalty is solely of a financial nature or where a financial penalty and a financial*



penalty of a non-pecuniary nature may be imposed but the second penalty is justified, voluntary payment by the person presumed to be liable, at any time prior to the decision, shall lead to the termination of the proceedings, except as regards the restoration of the situation which has been altered or the determination of compensation for the damage caused by the commission of the infringement.

3. In both cases, where the penalty is purely financial in nature, the body responsible for deciding the procedure shall apply reductions of at least 20 % of the amount of the penalty proposed, which are cumulative with each other. Such reductions shall be determined in the notification of initiation of proceedings and their effectiveness shall be subject to withdrawal or waiver of any administrative action or appeal against the penalty.

The percentage reduction provided for in this paragraph may be increased by regulation'.

The entity PAGE GROUP EUROPE, during the period granted to it to submit arguments on the proposal for the resolution, proceeded to voluntarily pay the penalty with the reduction provided for by law, which determines the end of the procedure and renounces any administrative action or appeal against the penalty.

Therefore, in accordance with the applicable legislation, the Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Declare the termination of proceedings PS/00003/2021 against PAGE GROUP EUROPE, S.L. for infringements of Articles 12 and 5.1 (c) of the GDPR, as set out in Articles 83.5 (b) and 83.5 (a) of that regulation respectively; in accordance with Article 85 of the LPACAP.

SECOND: Notify this resolution to PAGE GROUP EUROPE, S.L.

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with the provisions of (48.6) and (114.1) (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Law 29/1998 of 13 July governing the Administrative Jurisdiction, within two months of the day following notification of this act, in accordance with Article 46 (1) of that Law.

938-231221

Mar España Martí
Director of the Spanish Data Protection Agency

Summary Final Decision Art 60

Complaint

Administrative fine.

EDPBI:ES:OSS:D:2022:334

Background information

Date of final decision:	N/A
Date of broadcast:	23 February 2022
LSA:	ES
CSAs:	AT, BE, CY, DEBY, DEBE, DEMV, DENW, DERP, HU, IE, IT, NL, PL, PT
Legal Reference(s):	Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 5 (Principles relating to processing of personal data).
Decision:	Administrative fine
Key words:	Administrative fine, Data minimisation, Exercise of data subject rights, Identity verification, Lawfulness of processing, Principles relating to processing of personal data, Right of access.

Summary of the Decision

Origin of the case

The controller is a company based in the United Kingdom that is part of a business group dedicated to recruitment. In March 2018, the complainant opened an account on the website of the company and applied for a job through the services of its Dutch brand. Later on, the complainant requested access to her personal data. In order to grant access, the controller required the complainant to prove her identity by providing two of the following documents: passport, identity card or driving license showing the date of birth; social security or national insurance card; utility bill not older than 3 months. The data subject replied that this constituted excessive data processing and communicated her intention to lodge a complaint with the NL SA. Following this, the controller limited the conditions for granting access and required a copy of the data subject's identity card. The data subject then lodged a complaint, underlining that identity card had not been required for the creation of her account on the controller's website.

As the department responsible for managing access requests for continental Europe was found to be established in Spain, the ES SA was identified as the LSA. It received the aforementioned complaint on

3 March 2020 and on 10 November 2020, it issued a draft decision in which it considered that there was no infringement of the right of access. The PT SA and the DE SA raised objections that were taken into consideration by the LSA. It then drew up a revised draft decision and since none of the CSAs raised any objection, an agreement was reached. Consequently, on 29 June 2021, the LSA decided to initiate penalty proceedings against the controller.

Findings

The LSA identified that this claim by a specific data subject had revealed a general action by the controller that applied to all the other data subjects that were in the same situation as the complainant. For this reason, the LSA determined that the infringement lied in the general action taken by the controller, and not exclusively in the present case.

The LSA held that the verification of the identity of the applicant must be limited to cases in which the controller has ‘reasonable’ doubts as to the identity of the person. In order to confirm the identity of the data subject in such cases, Article 12 (6) GDPR allows to require “additional information”. The LSA also brought forward Recital 64 of the GDPR that gives the controller the possibility to use all ‘reasonable measures’ to verify the identity of data subjects. However, as the Agency pointed out, these rules do not require to provide an identification document, and an electronic signature might be equivalent to an ID card. In addition, it highlighted that the request for access was made from the same email account registered in the controller’s database, and hence it was not understandable how the company could have doubts about the applicant’s identity. The LSA determined that the controller had not justified the existence of a ‘reasonable doubt’ to identify the identity of the applicant. Contrary to the respondent’s argument that the identity verification scheme applied only to cases where there were doubts about the identity of the applicant, it was demonstrated that this scheme applied to all cases of exercise of rights of access and portability in general, without providing other means of verification, and without determining first if such reasonable doubts existed.

Furthermore, the LSA also raised the issue that the controller had less intrusive methods to check the identity of the data subject. The LSA also considered that the applicant’s contact details available to the controller provided enough guarantees to have complied with the re-quest received. Besides, the LSA highlighted that the strict requirements imposed to comply with the applicant’s request left it unanswered, so that the data subject chose to go to her national SA instead. Although on 27 August 2020 the right of access was finally granted after an express request from the LSA, the latter reminded that it cannot be expressed in the context of an administrative procedure. For the aforementioned reasons, it was considered that there was an infringement of Article 12 (2) and (3) of the GDPR, as a result of the failure to take account of the right of access exercised by the complainant.

The LSA also pointed out that there was not a guarantee that only personal data necessary for the verification of the identity was processed by the use of two out of the three documents required by the controller. Moreover, the LSA considered that this processing increased the risk for those concerned and did not guarantee a level of security appropriate to the risk. Besides, the LSA took into account the arguments raised by the two CSAs that made objections to the draft decision - it accepted that access to the data subject’s private account in the controller’s website should be considered as sufficient and encouraged less intrusive verification means of the identity. Hence, the LSA concluded that the identification system designed by the company did not meet any of the criteria and factors lied down in Article 25 (1) of the GDPR, such as the context, the risks or the purpose of the processing.

Therefore, the LSA considered that, in the cases where data subjects had provided them with the documentation required to satisfy requests for access or portability, the controller had processed inappropriate, irrelevant, and not necessary personal data. It held that this processing was contrary

to the principle of ‘data minimisation’ laid down in Article 5 (1) (c) GDPR, even though the controller rectified and required only the copy of the identity card, instead of the previous required documents.

Decision

On 24 November 2021, a motion for resolution was issued, penalising the controller for a minor infringement of Article 12 GDPR, with a fine of 50,000 EUR and for a very serious infringement of Article 5 (1) (c) GDPR, with a fine of 250,000 EUR. In addition, the LSA considered that the new means of validating the identity of applicants and the new procedures set to manage applications for the exercise of rights complied with the GDPR and it was not necessary to impose additional measures to the respondent. On 2 December 2021, the controller voluntarily paid the penalty making use of a reduction (240,000 EUR), thus terminating the procedure and waiving any administrative action or appeal against the penalty.

Procedure No: E/07781/2020
IMI Reference: Case Register 177442

FINAL DECISION TO DISCONTINUE PROCEEDINGS

From the actions carried out by the Spanish Data Protection Agency and based on the following

FACTS

FIRST: On 28 September 2020, the investigation was initiated as a result of an analysis of a letter notifying a personal data breach, sent by TEKA INDUSTRIAL, S.A with VAT A39004932 (hereinafter TEKA), informing the Spanish Data Protection Agency, on 24 August 2020, of the following: TEKA belongs to the HERITAGE-B group and has suffered a security breach resulting from a **ransomware attack** affecting various entities of the Group located in different countries, including TEKA. It also states that there are group companies in Germany, France, the United Kingdom, Switzerland and Mexico. The HERITAGE-B Group has notified the AEPD and the German Authority as it considers that they are the countries where the main establishments of the group are located.

SECOND: The 'Internal Market Information System' (hereinafter 'the IMI system'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information. Via the IMI system (A56ID 175553), on 20 January 2021 the Spanish Agency declared itself the lead authority in this case, pursuant to Article 4 (23) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), since TEKA has one of its main establishments in Spain.

According to the information entered into the IMI system, in accordance with Article 60 of the GDPR, act as concerned supervisory authorities in this case the supervisory authorities of: Berlin (Germany), Baden-Württemberg (Germany), Bavaria — Private sector (Germany), France and Mecklenburg-Western Pomerania (Germany). All of them under Article 4 (22) GDPR, given that data subjects residing in these Member States are substantially affected or are likely to be substantially affected by the processing at issue in these proceedings.

THIRD: The General Subdirectorate of Data Inspection carried out preliminary investigations in order to establish a possible infringement of data protection legislation, becoming aware of the following:

On 27 October 2020, information was requested from TEKA and the reply received shows the following:

With regard to the company

— TEKA is a company belonging to the HERITAGE-B corporate group which manufactures, sales and distributes products made from special steels. TEKA is the lead company in three distinct business lines: kitchens, baths and containers.

TEKA is considered to be the lead entity of the HERITAGE-B Group in so far as certain relevant decisions relating to information systems are taken by the HERITAGE-B Group.

— The Group's main provider is Microsoft Ireland Operations Limited, with whom TEKA has a framework service contract in the European region.

TEKA stated that the systems where the breach had occurred were maintained internally by the Group's IT teams.

With regard to the chronology of the events

— *On 3 August 2020, a suspicious activity began with the creation of an administrator account in the group's corporate systems.*

— *On 5 August the first suspicious behaviour appeared with several attempts to connect on the corporate network and the execution of the first malicious file.*

— *Tools and services are installed between 5 and 21 August 2020 using an interface and preparing the environment for further exploitation.*

— *On 21 August 2020 ransomware was implemented throughout the corporate network.*

TEKA states that the detection took place on 21 August and immediately activated a monitoring system (expert cybersecurity teams of Telefónica) to monitor the activity of the systems and detect, where appropriate, any other suspicious activity.

On the causes that made the security breach possible

— *The entrance of the attackers to TEKA's systems took place through the theft of user accounts by phishing and the discovery of passwords by gross force (testing and error of millions of combinations to gain access).*

Once within the corporate network, movements were detected using legitimate credentials of remote desktop applications.

Measures to minimise the impact of the security breach and actions taken for final resolution

— *On 21 August, TEKA closed the servers and isolated the systems to contain the cyber-attack and contracted Telefónica to carry out a forensic analysis of the incident.*

— Immediately, technical measures were taken at network level and other measures such as the retrieval and security of the servers concerned or the activation of existing backups.

— At the same time, Telefónica carried out constant real-time monitoring, carrying out, *inter alia*, the analysis of access records (log), system analysis and network traffic analysis.

Senior management, legal and IT teams were also involved in the incident analysis to create contingency plans and take appropriate measures in each business unit.

With regard to the data concerned

— The number of people affected is around 2.000, of which 569 are Spanish and the other countries of the European Union and third countries.

— The data affected by the Incident were mostly corporate data (TEKA's business is aimed at the sale of business-to-business products and services — business to business B2B — and therefore customers and suppliers are generally legal persons).

TEKA considers that the attack was not aimed at obtaining personal data but at business information.

The categories of data concerned are: basic identification data, ID card/NIE/passport, access or identification credentials, economic or financial data, contact details and business and company information.

— TEKA states that they have monitored the activity after the security breach and is not aware of any malicious use by the attackers.

However, the publication on the darkweb — on 16 September — of certain information affected by the incident was immediately identified and all links to the incident were quickly disabled, so it is estimated that the information was only accessible for the minimum time needed to disable those links (approximately 1 hour).

On 23 August, TEKA carried out a risk analysis in accordance with the model included in the Guide on the Management and notification of security breaches published by the AEPD, which concluded, on the basis of the technical and forensic information available on that date, that the incident did not pose a high risk to the rights of those affected, whereas the incident consisted mainly of encryption of data — mainly corporate — and the use of data by third parties had not been identified. TEKA therefore decided, on the basis of the available information, that there was no need to notify the data subjects about the incident.

— On 17 September, TEKA carried out a second risk analysis with more information and after it had been identified that certain data had been provided as a result of the incident and had been published on the darkweb in order to verify what action should be taken as a result of these findings.

On the basis of the information available on 17 September, TEKA determined that such exfiltration did not pose a high risk to the rights of those affected by Teka's business and activity in so far as the information published was mostly corporate and access to it had been prevented within 1 hour of its publication.

Notwithstanding the above, the analysis was made not only for TEKA but also for the other entities in the group. As a result of that analysis, certain German group entities affected by the incident (namely KEK GmbH, THIELMANN UCON GmbH and THIELMANN WEW GmbH) did determine, by the nature of the potentially compromised information concerning their organisations, that it was appropriate to notify those employees whose bank details had been compromised as a result of the incident in order to recommend them to take appropriate measures and avoid being subject to fraud or other similar criminal activity.

— **TEKA states that it aims to maintain a dynamic and continuous risk assessment (which takes into account the updated information at every stage of the process and is revised in the event of new findings), granular and detailed, which involves maintaining open lines of communication with the authorities, and a detailed analysis of whether or not it is necessary to communicate the security breach to data subjects in accordance with the AEPD and other authorities methodology, so that communication has been made in the relevant cases.**

With regard to security measures implemented prior to the security breach

— **TEKA has a strict policy against phishing and carries out frequent awareness-raising campaigns for its employees through informative emails, both preventive and warning against specific phishing attempts against the organisation on aspects of the company's technological use policy.**

The procedures provided to address such threats define the protocol to be followed for the notification and handling of such security incidents.

In that regard, TEKA has provided a copy of the explanatory emails on phishing and the protocol to be followed 'Protection against cyber-attacks'.

TEKA has also provided the document 'HERITAGE Group's Information Technology Use Policy'. This document contains the Annexes: 'IT Acceptance and Authorisation for Personal Devices Form'.

It includes, inter alia, the policy for passwords, internet usage and personal devices.

— **TEKA has provided the following documents:**

- **Copy of the Register of Processing Activities where the reported security breach has occurred.**
- **Security policy (HERITAGE Group's Information Technology Use Policy).**

- **Back-up manual.**
- **Procedure for the registration, removal and modification of user permits.**
- **Emails classification policy according to their level of protection**
- **Phishing protection policy.**
- **Register of access to the anonymised Data Processing Centre.**
- **Security breach management procedure**

With regard to measures implemented after the security breach

- **As a result of the incident, in order to strengthen its security measures and to be able to monitor its efficiency, TEKA has hired the company SECURE & IT to carry out a specific audit of the security elements of the Group. This company will also provide maintenance services to deal with incidents.**
- **Procurement of tools with Microsoft and the management and monitoring of these tools with certified partners similar to Telefónica.**
- **TEKA is currently reviewing and updating all its security measures, including its policies. The following measures have been taken after the Incident:**
 - **Strengthening access control**
 - **Complexity of passwords and shortening of the renewal period;**
 - **Sessions analysis on a more regular basis;**
 - **General prohibition of the use of personal devices (only allowed in exceptional cases);**
 - **Monitoring the use of unauthorised applications;**
 - **Use of authorised file sharing tools only**
- **Reinforcement of recommendations on sending sensitive information (personal data, confidential data, etc.) in encrypted attachments and, in general, security awareness campaigns among employees.**

Information on the recurrence of these events and the number of similar events occurring over time

- **TEKA has no evidence of a recurrence of facts relating to the incident.**

FOURTH: On 02 September 2021, the Director of the AEPD adopted a draft decision to discontinue the proceedings. On the same day, following the process set out in Article 60 of the GDPR, the draft decision to discontinue the proceedings was shared in IMI and

the concerned supervisory authorities were informed that they had four weeks from that time to raise relevant and reasoned objections. During the expiry of the period for that purpose, the concerned supervisory authorities did not raise relevant and reasoned objections in that regard, and therefore all the supervisory authorities were deemed to agree with and were bound by that draft decision, in accordance with Article 60(6) GDPR.

LEGAL GROUNDS

I Competence

In accordance with the powers of investigation and corrective powers conferred on each supervisory authority by Article 58 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), and in accordance with Article 47 of the Spanish Organic Law 3/2018 of 5 December 1995 on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is competent for deciding on these procedure.

II Preliminary remarks

Article 4.12 GDPR defines 'personal data breaches' (hereinafter "security breach") as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*'.

In the present case, it is common ground that there was a personal data security breach in the circumstances set out above, categorised as a confidentiality breach, as a result of a **ransomware attack affecting TEKA**.

It should be noted that reporting a personal data security breach does not entail the imposition of a penalty directly, as it is necessary to analyse the diligence of controllers and processors and the security measures applied.

The security of personal data is regulated by Articles 32, 33 and 34 GDPR, which regulate the security of the processing, the notification of a personal data security breach to the supervisory authority, as well as the communication to the data subject.

III Article 32 GDPR

Recital (39) of the GDPR states that:

'(...) 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'.

In this regard, Article 32 'Security of processing' of the 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 risks 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) pseudonymisation and encryption of personal data;*
- (b) the ability to ensure the ongoing 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;*
- (D) a process of regular verification, assessment and assessment of the effectiveness of technical and organisational measures to ensure the security of the 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.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and the processor shall take measures to ensure that any person acting under the authority of the controller or of the processor who has access to personal data may process such data only on instructions from the controller, unless required to do so by Union or Member State law."

'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) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the 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.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law'.

In the present case, prior to the security breach under consideration, TEKA already had a strict policy against phishing and carried out frequent awareness-raising campaigns for its employees by means of information emails, both preventive and warning of specific phishing attempts detected against the organisation on aspects of the company's technological use policy. Despite this, attackers were able to enter TEKA's systems through the theft of user accounts by phishing and the discovery of passwords by raw force (testing and mistake of millions of combinations to gain access).

While on 3 August 2020 started a suspicious activity with the creation of an administrator account in the Group's corporate systems, it is not until 21 August 2020 that ransomware is executed across the corporate network, which is when TEKA became aware that the security incident had occurred. On the same day, TEKA closed the servers and isolates the systems to contain the cyber-attack and contracted Telefónica to perform a forensic analysis of the incident. Technical measures were immediately taken at network level and other measures such as retrieval and securitisation of affected servers or activation of existing backups. At the same time, Telefónica carried out constant and real-time monitoring, carrying out, inter alia, the analysis of access records (log), system analysis and network traffic analysis. Senior management, legal and IT teams were also involved in the incident analysis to create contingency plans and take appropriate measures in each business unit.

As a result of the incident, TEKA has contracted SECURE & IT to carry out a specific audit of the Group's security features. This company will also provide maintenance services to deal with incidents.

Tools have also been contracted with Microsoft and commissioned the management and monitoring of these tools to certified partners similar to Telefónica.

In addition, TEKA is currently reviewing and updating all its security measures, including its policies, and the following measures have been taken:

- Strengthening access control;
- Complexity of passwords and shortening of the renewal period;
- Sessions analysis on a more regular basis;
- General prohibition of the use of personal devices (only allowed in exceptional cases);
- Monitoring the use of unauthorised applications;
- Use of authorised file sharing tools only
- Reinforcement of recommendations on sending sensitive information (personal data, confidential data, etc.) in encrypted attachments and, in general, security awareness campaigns among employees.



In the present case, it is not apparent from the documents provided by TEKA in the course of these investigations that, prior to the security breach, TEKA did not have reasonable security measures on the basis of the estimated potential risks.

Furthermore, there is no evidence that it did not act diligently once the security breach had been known, nor that the measures taken after the incident in question were inadequate.

There are also no complaints to this Agency from data subjects relating to the present security breach.

IV Article 33 GDPR

Recital (85) of the GDPR states that:

'A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.'

In that regard, Article 33 '*Notification of a personal data breach to the supervisory authority*' of the GDPR provides:

'1. 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.'

'2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.'

'3. The notification referred to in paragraph 1 shall at least:

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*

(c) describe the likely consequences of the personal data breach;
 (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.'

In the present case, TEKA notified the security breach within the period laid down in the GDPR for that purpose, with the information set out in Article 33 of the GDPR.

V
Article 34 GDPR

Recital (86) of the GDPR states that:

"The controller should communicate the personal data breach to the data subject without undue delay if it may result in a high risk to his or her rights and freedoms and allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate a risk of immediate damage would justify swift communication with data subjects, while it can be justified that communication takes longer because of the need to implement appropriate measures to prevent continuous or similar personal data breaches."

'The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication'

In this regard, Article 34 'Communication of a personal data breach to the data subject' of the GDPR provides:

"1. Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay. L 119/52 ES Official Journal of the European Union 4.5.2016

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has put in place appropriate technical and organisational protection measures and these measures have been applied to the personal data concerned by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken further steps to ensure that the high risk to the rights and freedoms of the data subject referred to in paragraph 1 is no longer likely to materialise; (c) involves a disproportionate effort. In such a case, there shall instead be a public communication or a similar measure whereby the data subjects are informed in an equally effective manner.

4. Where the controller has not yet communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach leading to a high risk, may require the data subject to do so or may decide that one of the conditions referred to in paragraph 3 is fulfilled."

'1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data

breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met’.

In the present case, the number of people affected is around 2.000, of which 569 are Spanish and the rest of the other countries of the European Union and third countries.

However, the data affected by the incident were mostly corporate data, as TEKA’s business is aimed at the sale of business-to-business products and services — business to business B2B — and therefore customers and suppliers are generally legal persons. In addition, TEKA considers that the attack was not aimed at obtaining personal data but at business information. On 23 August 2020, TEKA carried out a risk analysis in accordance with the model included in the Guide on the management and reporting of security breaches published by the AEPD, which concluded, on the basis of the technical and forensic information available on that date, that the incident did not pose a high risk to the rights of data subjects, whereas the incident mainly consisted of encryption of data — predominantly corporate — and the use of data by third parties had not been identified. TEKA therefore decided, on the basis of the available information, that there was no need to notify the data subjects about the incident.

Subsequently, TEKA identified on 16 September 2020 the publication on the darkweb of certain information affected by the incident and all links to the incident were quickly disabled, so it is estimated that the information was only accessible for the minimum time needed to disable those links (approximately 1 hour).

On 17 September 2020, TEKA carried out a second risk analysis with more information and found that such exfiltration did not pose a high risk to the rights of those affected by TEKA’s business and activity in so far as the information published was mostly corporate and access to it had been prevented within 1 hour of its publication.

However, the analysis was made not only for TEKA but also for the other entities in the group. As a result of that analysis, certain German group entities affected by the incident (namely KEK GmbH, THIELMANN UCON GmbH and THIELMANN WEW GmbH) did determine, by the nature of the potentially compromised information concerning their organisations, that it was appropriate to notify those employees whose bank details had been compromised as a result of the incident in order to recommend them to take appropriate measures and avoid being subject to fraud or other similar criminal activity.

In the present case, the security breach was not likely to result in a high risk to the rights and freedoms of natural persons, with the result that TEKA was not required to communicate to the data subjects that a security breach had occurred, within the meaning of Article 34 of the GDPR.

It should be noted that this AEPD has no complaints from potential victims.

VI

No infringement

Therefore, on the basis of the above paragraphs, no evidence has been found to prove the existence of an infringement within the remit of the Spanish Data Protection Agency.

In accordance with the above, the Director of the Spanish Data Protection Agency therefore:

AGREED TO:

FIRST: DISCONTINUE the present actions.

SECOND: Notify this decision to TEKA INDUSTRIAL, S.A.

In accordance with Article 50 of the Spanish LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with Article 114.1 (c) and with Articles 112 and 123 of Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, the parties concerned may lodge an appeal with the Director of the Spanish Data Protection Agency within one month of the day following notification of this decision or a direct administrative appeal to the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Spanish Law 29/1998 of 13 July governing the Administrative Jurisdiction, within two months of the day following notification of this act, as provided for in Article 46 (1) of that Law.

940-010921

Mar España Martí
 Director of the AEPD, P.O., General Subdirectorate of Data Inspection, [REDACTED]
 [REDACTED] Resolution 4 October 2021

File No: PS/00372/2021

IMI Reference: A56ID 122865- Case Register 128401

FINAL DECISION ON PENALTY PROCEEDINGS

From the actions taken by the Spanish Data Protection Agency and based on the following

BACKGROUND

FIRST: [REDACTED] (hereinafter the complainant) lodged a complaint with the Polish Data Protection Authority. The complaint is directed against GLOVOAPP23, S.. L. with VAT B66362906 ('GLOVOAPP'). The grounds on which the complaint is based are as follows:

Having discovered that his home was not within the scope of GLOVOAPP's riders (information which is only obtained once an account is opened and personal data entered), the complainant requested the deletion of his account and personal data, on two occasions with a difference of 5 days, but did not receive a reply. In addition, the forms available on the Glovo app for the revocation of consent are available only in Spanish, not in English or Polish.

In addition to the complaint, he provides:

— Copy of an email sent on 7 November 2019 at 0.10 hrs from *liveops.comms@glovoapp.com* to [REDACTED], with the following message: "*Thank you for contacting Glovo! We have just collected your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*". This email responds to a message dated 6 November 2019 at 23: 10 in which it is claimed that the delivery area is too small.

— Copy of an email sent on 12 November 2019 at 8:56 hrs from *liveops.comms@glovoapp.com* to [REDACTED], with the following message: "*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*". This email responds to a message dated 12 November 2019 at 8: 56 hrs explaining that his requests are not being dealt with. The complainant gives notice that he has already notified the Data Protection Authority and expects his account to be deleted immediately.

— Copy of an email sent on 12 November 2019 at 9:43 hrs from the email *liveops.comms@glovoapp.com* to [REDACTED], with the following message: '*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*'. This email responds to a message dated 12 November 2019 at 8: 43 hrs explaining that a week ago was sent an email requesting the deletion of his account and received no reply, but received an information document. He also warned that he would notify the

data protection authority that he did not have a request form for deletion of data in Polish, only in Spanish.

— Copy of an email sent on 13 November 2019 at 19:39 hrs from the email liveops.comms@glovoapp.com to [REDACTED], with the following message: “*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period*”. This email responds to a message dated 13 November 2019 at 18: 39 hrs requesting that his personal data should be immediately no longer processed and deleted from all databases. In addition, he requests the deletion of his account within two working days.

SECOND: On 27 April 2020, the Spanish Data Protection Agency (AEPD) received the complaint via the Internal Market Information System (hereinafter IMI), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), which aims to promote cross-border administrative cooperation, mutual assistance between Member States and the exchange of information. This complaint is forwarded to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR), taking into account its cross-border nature and that this Agency is competent to act as lead supervisory authority, given that GLOVOAPP has its registered office and main establishment in Spain.

This Agency agreed, on 18 May 2020, to be the competent authority to act as lead supervisory authority (LSA), in accordance with Article 56 (1) GDPR, as regards the right of erasure. However, it proposed to reject the part concerning the forms, as its inspection services checked that the data protection forms are downloaded in the language of the city selected on the homepage, and consequently the Polish forms are available if a Polish city is chosen.

The proposing authority raised the possibility to give the complainant the possibility to submit evidence that the forms were only available in Spanish at the time of the submission of the complaint, as the findings of the AEPD contested the complainant's complaint at the time the check was carried out (i.e. five months after the submission of the complaint). They commented that they would send a letter to the complainant requesting such a remedy, and that if they did not receive a reply within 7 days, they would accept the rejection of that part of the complaint.

On 11 August 2020, this Agency received an email from the Polish authority, informing that no reply had been received from the complainant, and that, as a result, the part of the complaint relating to the forms was dismissed, which was reduced to the issue related to the exercise of the right to erasure (Article 17 GDPR).

According to the information entered into the IMI system, pursuant to Article 60 of the GDPR, it acts as a ‘supervisory authority concerned’, in addition to the Polish data protection authority, the supervisory authorities of Portugal, Italy and France. All of them under Article 4 (22) GDPR, since data subjects residing in these Member States are likely to be substantially affected by the processing at issue in these proceedings.

THIRD: In accordance with Article 65 (4) of Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (hereinafter LOPDGDD), GLOVOAPP was informed of this complaint so that it could analyse it and inform this Agency within one month, of the measures taken to comply with the requirements laid down in the data protection legislation.

The request, which was carried out in accordance with the rules laid down in Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('LPACAP'), was recorded on 20 August 2020 as stated in the acknowledgement of receipt in the file.

On 18 September 2020, the Agency received a letter of reply stating:

- The origin of the incident lies in the fact that, contrary to what the complainant indicates, his personal data was not requested to be erased using the form provided for that purpose on the web portal, but by means of a chat with an agent of customer care service (SAC) in charge of management of orders and related incidents. Instead of using the various visible, clear and specific channels made available by the company, both on its website and in its application, to exercise his personal rights, i.e. the addresses *legal@glovoapp.com* and *gdpr@glovoapp.com*, as well as the different rights exercise forms published on the website and accessible in the application in the 'Contact' section, he requested the erasure of his data by means of an incorrect channel, not intended for this purpose.
- They state that their SAC assigns an agent responsible for answering users depending on the territory in which the user is located, in order to be able to reply in the same language as that in which the request is launched. In this case, the complainant was not assigned any city or territory since, as he had not placed an order via the app, he could not be located on the basis of the territory. This is why, in view of the fact that it was impossible to locate the user in a particular city, the system did not transmit the requests for erasure of data to any SAC actor, and the user received only the response that the SAC automatically generates before an agent responsible for responding to users is assigned.
- Following the transfer of the complaint, they have erased the complainant's personal data (clarify that they only had their email address, as he did not have any orders), and have contacted him to inform him of this, and of the retention of his data in a blocked state, inter alia, in order to defend themselves in complaints (they provided a copy of the email dated 16 September 2020). They explain that the reason for not having complied with his request was the use of an incorrect channel to exercise his right.
- In order to avoid such incidents occurring in the future, they have sent a reminder to all agents about the need to send to the Office of the Data Protection Officer all communications that may include a request for the exercise of rights, even if this request is hidden or not obvious. They have also reported to the SAC department the inconvenience related to the allocation of requests by users who have not placed orders or who have not indicated a country or address when registering in the app. As long as a technical solution to the problem is not found,

its staff shall monitor, manually and periodically, applications which have not been automatically assigned to any staff member.

- They also disagree with the fact, reported by the complainant, that forms are not available in their language, and also that it is necessary to open an account in order to know the geographical area of availability of service, since the coverage of mailings is accessible via a dedicated URL (<https://glovoapp.com/es/map> in Spain, for example).

FOURTH: On 11 December 2020, pursuant to Article 65 of the LOPDGDD, the complaint lodged by the complainant was declared admissible.

FIFTH: On 5 October 2020, the Director of the AEPD adopted a draft decision to discontinue the proceedings. Following the process set out in Article 60 GDPR, this draft decision was submitted via IMI on the same day and communicated to the concerned supervisory authorities that they had four weeks from that date to raise relevant and reasoned objections. Within the time limit set for that purpose, the Polish supervisory authority submitted its relevant and reasoned objections for the purposes of Article 60 of the GDPR, in the sense that it considered that there was no need to discontinue the proceedings but rather to analyse the case and issue a reprimand given that there had been an infringement of the GDPR. For its part, the Portuguese supervisory authority submitted its relevant and reasoned objections in the same sense, taking the view that GLOVOAPP should be penalised for an infringement of the GDPR.

SIXTH: On 3 September 2021, the Director of the AEPD adopted a revised draft decision initiating penalty proceedings. Following the process set out in Article 60 of the GDPR, this revised draft decision was transmitted via IMI on 6 September 2021 and the authorities concerned were informed that they had two weeks from that time to raise relevant and reasoned objections. Within the period for that purpose, the supervisory authorities concerned did not raise relevant and reasoned objections in that regard, so that all the supervisory authorities are deemed to agree with and are bound by that revised draft decision, in accordance with Article 60(6) GDPR.

SEVENTH: On 31 March 2022, the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against GLOVOAPP, in accordance with Articles 63 and 64 of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations ('the LPACAP'), for the alleged infringement of Article 12 of the GDPR, in conjunction with Article 17 of the GDPR, as set out in Article 83 (5) of the GDPR.

The initial agreement was notified in accordance with the rules laid down in the LPACAP on 11 April 2022, as stated in the acknowledgement of receipt in the file.

EIGHT: On 19 April 2022, GLOVOAPP submitted a letter requesting an extension of the deadline for submitting arguments.

NINTH: On 21 April 2022, this Agency decided to extend the time limit to a maximum of five days, in accordance with Article 32 (1) of the LPACAP.

The extension agreement was notified to GLOVOAPP on the same day, as stated in the acknowledgement of receipt in the file.

TENTH: On 3 May 2022, this Agency received a letter in due time and form from GLOVOAPP in which it put forward arguments on the decision to initiate the procedure, in which it stated, in summary, that:

FIRST. ON GLOVO'S COMPLIANCE WITH PERSONAL DATA PROTECTION RIGHTS

First, GLOVOAPP refers to the statements presented in the letter dated 18 September 2020 concerning the events concerning the management of the right to erasure exercised by the former user of Glovo, a Polish national, through the chat managed by Glovo's Customer Care Service Department (SAC).

In those statements, GLOVOAPP understands that it was clear that, at no time, Glovo refused or hindered the exercise of the complainant's right to erasure for the purposes of Article 12.2 of the LOPDGDD, but rather that Glovo showed flagrant flexibility by deleting the complainant's personal data immediately after receiving the complaint from this Agency, despite not being exercised through the channels authorised for that purpose at that time (email addresses *legal@glovoapp.com* and *gdpr@glovoapp.com*).

GLOVOAPP also refers to the reasons why GLOVOAPP was unable to delete the complainant's personal data in due time (it was impossible to locate it in a specific territory or city because he had not placed an order via the platform and, consequently, it was impossible to assign his request to a specific agent of the SAC), which cannot, in any event, be understood as an intention on the part of Glovo not to comply with its duty of care to the complainant's right to erasure, for the purposes of Article 74 (c) of the LOPDGDD.

Moreover, GLOVOAPP notes that the complainant's right to erasure was immediately respected for the reasons already expressed in the letter of 18 September 2020, supplemented by a massive sending to all the agents who are members of the SAC reminding them of the need to immediately refer to the Data Protection Officer any exercise of rights that might be reached through the chat.

It is therefore clearly demonstrated that GLOVOAPP, as a controller, was already insured and continues to ensure in its internal policies the satisfaction of data subjects' rights, regardless of how they are exercised.

It states that GLOVOAPP regularly and constantly monitors all the channels it has contact with the user (web forms, app chat, email address, post, social media profiles, etc.) in such a way that, if a data protection right is exercised, it is properly respected.

It considers that evidence of this is that, since the complainant's complaint sent by this Agency, GLOVOAPP has not received any other complaint from the latter or from any other supervisory authority in the countries in which it operates for failure to comply with a right to data protection and, in particular, a right to erasure. And that all these actions by GLOVOAPP cannot be understood in any other way than as a clear willingness on the part of GLOVOAPP to comply with the rules on the protection of personal data.

In the light of the above, GLOVOAPP considers that the Agency should not finalise it with a reprimand, since the actions that have taken place cannot be understood as a clear intention to breach the data protection rules in the way that they do not wish to comply with the complainant's right to erasure, and the proceedings should be closed.

SECOND. — ON THE AGENCY'S DECISION ON THE CLOSURE OF THE PROCEEDINGS

GLOVOAPP makes express reference to the decision of 5 October 2020 by which the Director of the AEPD adopted a draft decision to discontinue these proceedings.

While the concerned supervisory authorities of Poland and Portugal raised objections to the draft decision, it is clear to GLOVOAPP that the draft decision is not adopted by the AEPD without considering that the actions and evidence obtained so far do not result in the existence of a breach or serious harm to the rights and interests of the complainant.

GLOVOAPP considers that the AEPD, as the lead supervisory authority in these proceedings, should have maintained the decision taken at the time, being the reprimand an unnecessary and inappropriate sanction for this case, since Glovo has never shown a willingness not to comply with the complainant's right to erasure, especially since it has shown clear and unequivocal flexibility by deleting his data immediately after receiving the complaint from the AEPD, despite the fact that this right has been exercised by a channel not authorised for this purpose.

In short, GLOVOAPP considers that Glovo has not failed to comply with data protection rules, which is why the closure of the proceedings is the most appropriate decision for this case.

THIRD. — NULLITY OF THE ADMINISTRATIVE ACT ON THE GROUND THAT THE INFORMATION NECESSARY TO ESTABLISH AN INFRINGEMENT IS LACKING

In addition, GLOVOAPP considers that in no case can Glovo's conduct be sanctioned in the form of a reprimand, for the reasons set out below.

3.1 Absence of subjective elements of the infringement. Nullity of penalty

GLOVOAPP takes the view that it is necessary, first of all, to examine whether or not the essential elements and conditions necessary for the imposition of a penalty in this case have been met.

Thus, the principles governing the administration's power to impose penalties will be, in general, those of administrative sanctioning law and, in particular, 'the principles of legality, criminality, liability, proportionality and non-participation'.

Law 40/2015 of 1 October 1992 on the Legal Regime for the Public Sector provides that an administrative offence is an action, understood in the broad sense of any action — or omission by persons seeking to produce a result — and which the Legislator itself has classified as an infringement.

In accordance with the above, in order to be faced with a personal data protection infringement, there must have been an intentional or negligent act or omission of any degree of negligence. What does this mean? That the person liable could, at the very least, have required different conduct.

Without wishing to subscribe to a compendium of sanctioning law, we can define subjective elements of the type such as the different degrees of voluntary nature or, at the very least, failure to comply with due diligence; deception is the clear manifestation of the voluntary nature of the typical action in the commission and mere negligence is the conduct that lacks the necessary care in complying with health obligations.

Thus, it is for the competent body to examine whether the conduct under examination is intentional or negligent, since such an assessment is essential in order to be able to impose a penalty, since they are constituent elements of the administrative offence.

The case-law that could be cited in support of the above statement would be almost unlimited, so we will only refer to the judgment of the National High Court of 13 October 2005, since it gives a detailed overview of the principles of penalties, their development and the evolution of the applicable case-law criteria.

Given that the judgment referred to is rather lengthy, and in order not to prolong us unnecessarily by transcribing verbatim the entire content of the judgment, we can only extract the paragraphs that we consider to be most representative:

'Fourth... the assessment of guilt in the conduct of the offender is a requirement which arises directly from the constitutional principles of legal certainty and legality, as regards the exercise of powers to impose penalties of any kind. The principle of guilt is a basic element in classifying a person's conduct as punishable, i.e. it is an essential element in any administrative offence (...)

Sixth (...) In summary, guilt must be as proven as the active or negligent conduct penalised, and that evidence must be extended not only to the facts determining liability but also, where appropriate, to those which qualify or aggravate the offence. (...)'

It is precisely the analysis of guilt which distinguishes a system of strict liability, in which it is penalised solely on the basis of the result, from one based on the principle of fault.

GLOVOAPP therefore understands that it can be concluded that the agreement notified to GLOVOAPP ignores one of the essential elements when it comes to being able to impose a penalty (even in the form of a reprimand), such as the examination of guilt, it being fully demonstrated that GLOVOAPP did not at any time intentionally wish to disregard the complainant's right to erasure. The opposite is true. Glovo immediately drew attention to that right once it had been transferred by that agency.

GLOVOAPP therefore states that it must be borne in mind that the AEPD should have carried out this analysis and that, therefore, it cannot be established that Glovo intended to infringe the data protection legislation (in the way that it wished to hinder, prevent or not comply with the complainant's right to erasure), and that the assessment of that intention as an essential element of the administrative offence was disregarded. GLOVOAPP takes the view that the imposition of a penalty would be null and void.

3.2. The absence of evidence rebutting Glovo's presumption of innocence. Nullity of penalty

In this regard, it should be noted that, as it has been repeatedly pointed out by the case-law, the existence of conduct constituting an administrative offence is a prerequisite and inexcusable for the imposition of any administrative penalty. The administration cannot therefore penalise without sufficiently proving the guilt of the person penalised, that is to say, the existence of bad faith in its conduct. It is therefore clear that the administration bears the burden of proving the guilt of the person concerned, which must be proved by any of the means permitted under the law.

However, in the present case, GLOVOAPP is not aware that there is absolutely no evidence to support the rebuttal of the presumption of innocence which, within the administrative and sanctioning sphere, is fully applicable to relations between the administration and those administered, as has been recognised by countless judicial decisions in all hierarchical and territorial areas.

In this regard, for example, the judgment of the High Court of Justice of 10 June 1994 stated: '*(...) in the exercise of the power of the public authorities to impose penalties, the presumption of innocence of any person accused of an offence is, to the fullest extent possible, a presumption of innocence until proven guilty. This principle, incorporated in Article 24 of our Constitution, has the immediate procedural consequence of shifting the burden of proof to the accused, and in the case of the power to impose penalties, to the public administration. In adversarial proceedings, with the participation and hearing of the accused, it is for the defendant to provide, collect and produce the evidence, using common means to support the factual situation which it is claimed to be classified as an administrative offence. If no such evidentiary activity has taken place, it is clear that the account or description of the events by the authority or its staff does not give rise to a presumption of veracity which would oblige the accused to prove his innocence, thereby reversing the burden of proof*

 (SSTS of 16 December 1986 and 26 December 1988)

Similarly, in relation to this lack of evidence and for the purposes of assessing what happened in the present case, the judgment of the Supreme Court of 26 December 1983 (RJ 1983\ 6418), which provided as follows: '*(...) In matters relating to penalties, it is not sufficient for the Administration to believe that a person has carried out certain facts in order to apply the penalty applicable to them. Rather, it is necessary to establish that he is indeed the author of those acts, and this requirement cannot be considered to have been complied with by two reports, which (...) are no longer a subjective assessment of the person who issued them and that, even if the person who issued them is enhanced by the status of the author, it cannot be the decisive factor that the Administration seeks, when the person concerned contradicts it in full detail, and when it relates to facts which, by their very nature, could have been easily and definitively proven or confirmed by the most varied means (...). In the area of penalties under administrative law, it is not appropriate to rely on reasonable grounds, or conscientious assessments, in order to establish an administrative offence, by imposing on the administration which accuses and penalises, under the presumption of innocence, the burden of proving the truth of the acts he accuses, and that those facts are imputable to the accused person, given that the presumption of innocence referred to above, now enshrined in Article 24 of the Constitution, can only be rebutted by proof of guilt*' (SSTS of 16 February, 23 March and 28

September 1982 (RJ 1982/968, RJ 1982/2324 and RJ 1982/5513), the legality of administrative penalties is conditioned by the nature of the offence and the penalty and by the conclusive and unequivocal proof that the person penalised is responsible for it, recalling the Chamber's Supreme Court of 23 December 1981 (RJ 1981/5453) that the prosecution, in particular, of an administrative decision finalising corrective or penalty proceedings must be based on the analysis of the facts or act challenged, of its nature and scope, in order to determine and see whether or not the administrative offence pursued can be subsumed in one of the cases, the types of administrative offence provided for in the legislation which serves as the basis for estimating the infringement sought and, where appropriate, punished, a prosecution which must be carried out on the basis of a purely legal criterion, since the classification of the administrative offence is not a discretionary power of the administration or of the sanctioning authority, but rather a legal activity which requires, as an objective condition, the offence to be included in the predetermined legal category as a fault, the liability for an administrative offence cannot be resolved on the basis of mere presumptions, indicia or conjecture, but on the basis of the reality of facts that are fully established and proven (...).'

In those circumstances, it is clear that the Agreement should be required to go beyond the mere reference to the legal provisions of the LOPDGDD to which reference has been made above. In the present case, GLOVOAPP takes the view that the AEPD confines itself to reviewing the background to the file in the Agreement, but, as has been demonstrated, it can in no way be said that we are faced with a clearly intentional infringement of the data protection legislation by Glovo, especially if, as has been shown in the facts, the complainant's right to erasure was clearly respected.

In the view of GLOVOAPP, the main objective of the penalty proceedings must be to break the presumption of innocence enjoyed by any person required by seeking the intentional element in his action, the subjective element of the administrative offence by means of an evidentiary activity that can be considered sufficient.

However, GLOVOAPP considers that in the present case there is no real incriminating evidence in the initiation of proceedings to suggest that GLOVOAPP's conduct is culpable.

In the light of all the above arguments, GLOVOAPP asked the AEPD to withdraw the agreement imposing a penalty imposed on GLOVOAPP, on the grounds that it wished to be imposed with a total absence of evidence of guilt and, consequently, in breach of the fundamental right to the presumption of innocence enshrined in the Spanish Constitution.

3.3. Absence of guilt. Nullity of penalty

In order to prove the absence of guilt, GLOVOAPP refers, with regard to the invocation of the principle of guilt, that the Constitutional Court has established as one of the basic pillars for the interpretation of administrative sanctioning law that the principles and guarantees present in the area of criminal law are applicable, with certain nuances, in the exercise of any power to impose penalties on the part of the public administration (STC 76/1990 of 26 April 2007).

In its judgment of 10 February 1986, the Supreme Court stated that '*the exercise of the power to impose penalties, whatever its manifestations, must be consistent with the constitutional principles and requirements governing the criminal legal system as a whole, and, whatever the sphere in which the State's punitive power, the courts, or the field in which it occurs, are subject to the same principles, the observance of which legitimises the imposition of penalties and penalties. therefore, administrative offences must, in order to be punishable or punished, be typical, that is to say, provided for as such by previous legal rules, which are unlawful, that is to say, damage to a legal asset provided for by law, and culpable, attributable to an perpetrator on the basis of willful misconduct or fault, in order to ensure, in his assessment, the balance between the public interest and the guarantee of individuals, which is the key to the rule of law'*'.

In the specific case, at no time has GLOVOAPP failed to comply with the data protection rules, and GLOVOAPP considers that it has fulfilled all its obligations in a religious manner. There has been no intention to infringe, quite the contrary.

GLOVOAPP considers that it has demonstrated to the AEPD its willingness to comply with the rules on the protection of personal data by immediately deleting the complainant's data once the complaint has been forwarded by the AEPD and ensuring that users' rights are fully satisfied at all times regardless of the channel they are exercised.

For all the above arguments, GLOVOAPP considers that there is a complete absence of evidence of guilt and, consequently, a violation of the fundamental right to the presumption of innocence enshrined in the Spanish Constitution.

3.4. Absence of the principles of criminality and presumption of innocence. Nullity of penalty

GLOVOAPP considers it necessary to highlight the non-existence of the conduct found to constitute an infringement and for which it is penalised in administrative proceedings.

This should have led the AEPD to close the penalty proceedings against GLOVOAPP (decision already taken by the AEPD in its draft decision of 5 October 2020), since otherwise there would be a flagrant breach of the principle of criminality resulting from the applicable legislation.

It has already been stated, in principle, that the legal system protects those involved in penalty proceedings by requiring that the administrative bodies responsible for the initiation of penalty proceedings consider as infringements only conduct that adequately falls within the definitions that explicitly establish rules with legal status. Thus, the first paragraph of Article 129 of Law 40/2015 provides as follows: '**Article 27. Principle of criminality. 1. Administrative offences are only infringements of the legal order provided for as such by a law, without prejudice to the provisions of Title XI of Law 7/1985 of 2 April 1992 for the Local Government**' (emphasis added and bold).'

In close connection with that provision, Law 40/2015 provides that the starting point for any action aimed at establishing liability for the commission of administrative offences must be to consider that, unless it is established otherwise, the person concerned has not committed the types declared as such.

As mentioned above, this is known as the principle of the presumption of innocence, which is fully consistent with the fact that the administration is obliged to carry out the investigative activity in order to verify whether specific conduct is subsumed into a type of infringement. Thus, with regard to the presumption of innocence, Law 39/2015 provides that that principle also applies to penalty proceedings.

With regard to the importance of compliance with the principle of criminality in the administrative procedure, the judgment of the Supreme Court of 2 June 2010, Chamber for Contentious Administrative Proceedings, Section 4, stated, and reproduced in extensive and consolidated legal literature, the following: '*The principle of criminality, the most important of those on which the right to impose an administrative penalty is based, requires, at the very least, a perfect match between the act and the final act as a breach, such as the objective and personal circumstances which determine the illegality, in order to establish precisely the conduct of the person concerned at the definitive rate by the provision deemed to have been breached (judgments of 25 March 1977, 13 May and 22 December 1986). Judgments of the Tribunal Supremo (Supreme Court) of 12 February).*'

As regards the principle of the presumption of innocence in the context of administrative powers to impose penalties, the case-law has also been unequivocal in that it requires administrative bodies to comply strictly with and subject to it. Thus, from an early stage — and settled case-law — the Constitutional Court has consistently held that the principle of the presumption of innocence fully subjects the power to impose administrative penalties.

As an example, reference may be made — for example — to Judgment of the Constitutional Court 13/1982 of 1 April 2007, which was expressed verbatim as follows: '*(...) the presumption of innocence is no longer a general principle of the right to be informed by judicial activity ("in dubio pro reo") in order to become a fundamental right which is binding on all public authorities and which is applicable immediately, as the Court has stated in numerous judgments.... The right to the presumption of innocence cannot be understood as being limited to the strict scope of prosecution of allegedly criminal conduct, but must also be understood as leading to the adoption of any decision, whether administrative or judicial, which is based on the status or conduct of the persons and which results in a penalty for them or limiting their rights.*'

In greater detail, the Supreme Court has also enshrined in its judicial activity the application of the principle of the presumption of innocence. Thus, by judgment of 28 February 1994, Chamber for Contentious Administrative Proceedings, Section 7, the High Court held: '*From a broad perspective, the identity of the principles of administrative sanctioning law with the power to impose criminal penalties is limited to the following general doctrines: the principle of legality (there is no administrative offence or penalty without any prior law determining them), the principle of typical unfairness (specific delimitation of the conduct to be criticised for the purposes of the penalty), the principle of 'nulla punición sine culpa' (the existence of intent or fault on the part of the perpetrator of the offence subject to the condition of a penalty) and, finally, with obvious significance in the present case, the principle of full proof of the reality of the impugned conduct, the expression of which in the constitutional principle of the presumption of innocence is clear, and which is sufficient to prove the actual performance by the accused of the*

impugned act or omission, with strict application of the right to impose administrative penalties'.

In view of the importance which the legal system attaches to the principles of criminality and the presumption of innocence in the context of the administration's power to impose penalties, and given the extensive acceptance in the case-law of the obligation to apply those principles to the administrative penalty procedure, all of the foregoing must be compared immediately with what happened in the present proceedings.

In the light of the above, GLOVOAPP considers that it has been duly demonstrated that it has always acted in good faith, applying the utmost effort to comply with data protection rules in the belief that it is lawful, as this is its requirement as a controller of the personal data of data subjects and with the aim of never jeopardising their rights and freedoms. There is therefore no clear 'intent' in failing to comply with the legislation in force, since it took all the necessary and appropriate actions to comply with the rules and has prudently aligned its actions with the law.

ELEVENTH: On 9 May 2022, the body conducting the penalty proceedings issued a proposal for a resolution, in which it proposed that the Director of the AEPD issue a reprimand to GLOVOAPP23, S. L., VAT B66362906, for an infringement of Article 12 of the GDPR, as set out in Article 83 (5) of the GDPR.

The proposal for a resolution was notified in accordance with the rules laid down in the LPACAP on 18 May 2022, as stated in the acknowledgement of receipt in the file.

TWELFTH: After the deadline for this purpose, we have not received any comments from GLOVOAPP on the above-mentioned proposal for a resolution.

The actions taken in these proceedings and the documentation contained in the file have shown the following:

PROVEN FACTS

FIRST: On 7 November 2019 at 0.10 hrs an email was sent from liveops.comms@glovoapp.com to [REDACTED] with the following message: '*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period.*' This email responds to a message dated 6 November 2019 at 23: 10 in which it is claimed that the delivery area is too small.

SECOND: On 12 November 2019 at 8: 56 hrs an email was sent from liveops.comms@glovoapp.com to [REDACTED] with the following message: '*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period.*' This email responds to a message dated 12 November 2019 at 8: 56 hrs explaining that his requests are not being dealt with. The complainant notes that he had already notified the Data Protection Authority and he expects his account to be deleted immediately.

THIRD: On 12 November 2019 at 9:43 hrs an email was sent from *liveops.comms@glovoapp.com* to [REDACTED] with the following message: '*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period.*' This email responds to a message dated 12 November 2019 at 8: 43 hrs explaining that a week ago he sent an email requesting the deletion of his account and received no reply, but received an information document. He also warned that he would notify the data protection authority that they did not have a request form for deletion of data in Polish, only in Spanish.

FOURTH: On 13 November 2019 at 19:39 hrs an email was sent from *liveops.comms@glovoapp.com* to [REDACTED] with the following message: '*Thank you for contacting Glovo! We have just received your message. We will respond to it in 24 hours. Thank you for your patience during this waiting period.*' This email responds to a message dated 13 November 2019 at 18: 39 hrs requesting that his personal data be immediately no longer processed and deleted from all databases. In addition, he requests the deletion of his account within two working days.

FIFTH: The Client Care Service (SAC) of GLOVOAPP allocates a user response agent depending on the territory in which the user is located, in order to be able to respond in the same language as the one in which the request is launched. In this case, the complainant was not assigned any city or territory, as he had not placed an order through the app and could not be located on the basis of the territory. This is why, since it was impossible to locate the user in a particular city, the system did not transmit the data deletion requests to any SAC actor, and the user received only the response that the SAC automatically generates before a user response agent is assigned.

SIXTH: Following the transfer of the complaint, GLOVOAPP has deleted the complainant's personal data (although they only had his email address, as he did not make any order), and have contacted him to inform him of this, and of the retention of his data in a blocked state, *inter alia*, to defend himself in complaints (by email dated 16 September 2020).

SEVENTH: GLOVOAPP has sent a reminder to all actors on the need to send to the Office of the Data Protection Officer all communications that may include a request to exercise rights, even if this request is hidden or not obvious. It has also reported to the department responsible for the SAC the inconvenience related to the allocation of requests by users who have not placed orders or who have not indicated a country or address when registering in the app. As long as a technical solution to the problem is not found, its officers will check, manually and regularly, requests that have not been automatically assigned to any actor.

LEGAL GROUNDS

I
Competence and applicable law

In accordance with the powers conferred on each supervisory authority by Article 58 (2) of Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)), and in accordance with Articles 47 and 48.1 of Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is responsible for initiating and deciding on this procedure.

In addition, Article 63(2) of the LOPDGDD provides that: "*The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures*".

II Preliminary remarks

In the present case, in accordance with Article 4 (1) of the GDPR, there is a processing of personal data, since GLOVOAPP collects and stores, as a minimum, the electronic mail of natural persons, among other processing operations.

GLOVOAPP carries out this activity in its capacity as controller, since it is the controller who determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR.

The GDPR provides, in Article 56 (1), for cases of cross-border processing, as provided for in Article 4 (23) thereof, in relation to the competence of the lead supervisory authority, that, without prejudice to Article 55, the supervisory authority of the main establishment or 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 set out in Article 60. In the case under consideration, as explained above, GLOVOAPP has its main establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

The right to erasure of personal data is regulated by Articles 17 of the GDPR and Article 15 of the LOPDGDD, while the way in which these rights are to be respected is regulated in Article 12 GDPR.

III Allegations

With regard to the allegations in response to the decision to initiate the present penalty proceedings, we will respond to them in the order set out by GLOVOAPP:

FIRST. ON GLOVO'S COMPLIANCE WITH PERSONAL DATA PROTECTION RIGHTS

GLOVOAPP understands that it became apparent that at no time did it deny or impede the exercise of the complainant's right to erasure for the purposes of Article 12.2 of the LOPDGDD, but rather showed flagrant flexibility by deleting the complainant's personal data immediately after receiving the complaint from this Agency, despite not being

exercised through the channels authorised for that purpose at that time (email addresses legal@glovoapp.com and gdpr@glovoapp.com).

In addition, it refers to the reasons why it was unable to delete the complainant's personal data in due time (it was impossible to locate it in a specific territory or city because it had not placed an order via the platform and, consequently, it was impossible to assign its request to a specific agent of the SAC), which cannot in any event be understood as an intention on the part of GLOVOAPP not to comply with its duty of care for the right of deletion exercised by the complainant, for the purposes of Article 74 (c) of the LOPDGDD.

Moreover, GLOVOAPP notes that the complainant's right to erasure was immediately respected for the reasons already expressed in the letter of 18 September 2020, supplemented by a massive sending to all the agents who are members of the SAC reminding them of the need to immediately refer to the Data Protection Officer any exercise of rights that might be reached through the chat.

It is therefore clearly demonstrated that GLOVOAPP, as a controller, was already insured and continues to ensure in its internal policies the satisfaction of data subjects' rights, regardless of how they are exercised.

In that regard, the Agency would like to point out that it was precisely not 'ensured' that the rights of data subjects would be satisfied, irrespective of the way in which they are exercised, since the complainant requested the deletion of their data via a channel which was certainly different from that provided for by GLOVOAPP, which is why the company was unable to comply with it correctly. This was, as the company acknowledges, due to the fact that the complainant had not placed an order, so that it could not be allocated a specific territory or city, which caused it not to be assigned a specific agent of the SAC to that request.

Although it is true that, after the complaint was forwarded by this Agency, GLOVOAPP has duly complied with the complainant's request, which is positively assessed by this Agency, the fact remains that the complainant's request was not complied with within the time limit laid down by the GDPR.

GLOVOAPP also maintains that it regularly and constantly monitors all the channels with which it has contact with the user (web forms, app chat, email address, post, social media profiles, etc.) so that, if a data protection right is exercised, it is properly respected.

This is demonstrated by the fact that, since the complainant's complaint sent by this Agency, GLOVOAPP has not received any other complaint from the latter or from any other supervisory authority in the countries in which it operates for failure to comply with a right to data protection and, in particular, a right to erasure.

However, this Agency would like to stress that the fact that no other complaint has been received from any supervisory authority does not constitute evidence that it 'monitors regularly and constantly all the channels with which it has contact with the user (...) in such a way that, if a data protection right is exercised, it is properly respected'.

In any event, it is clear that, irrespective of the action taken by GLOVOAPP after the facts at issue in these proceedings, at the time when the complainant made his request to delete his data, this monitoring was not being carried out or was not being carried out correctly, given that his right was not properly respected.

Finally, GLOVOAPP considers that the Agency is finalising it with a reprimand, but the actions that have taken place cannot be understood as a clear intention to breach the data protection rules in the way that they do not wish to comply with the complainant's right to erasure, and that they should be closed.

In this regard, the Agency does not consider that there was a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received via channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case.

In the light of the above, the present claim is rejected.

SECOND. — ON THE AGENCY'S DECISION ON THE CLOSURE OF THE PROCEEDINGS

GLOVOAPP makes express reference to the decision of 5 October 2020 by which the Director of the AEPD adopted a draft decision to discontinue these proceedings.

While the concerned supervisory authorities of Poland and Portugal raised objections to the draft decision, it is clear to GLOVOAPP that the draft decision is not adopted by the AEPD without considering that the actions and evidence obtained so far do not result in the existence of a breach or serious harm to the rights and interests of the complainant.

GLOVOAPP considers that the AEPD, as the lead supervisory authority in these proceedings, should have maintained the decision taken at the time, the reprimand being an unnecessary and inappropriate sanction for this case, since Glovo has never shown a willingness not to comply with the complainant's right to erasure, especially since it has shown clear and unequivocal flexibility by deleting his data immediately after receiving the complaint from the AEPD, despite the fact that this right has been exercised by a channel not authorised for this purpose.

In this respect, the Agency would like to point out that the mechanism that Article 60 GDPR obliges the lead authority, in the case of cross-border processing, to take a unanimous decision together with the other authorities concerned. It is precisely envisaged that a new decision will be reached in which all supervisory authorities agree, either by means of a draft decision or a revised draft decision.

In this regard, the Spanish Agency initially proposed to the other authorities that the proceedings be discontinued by means of the aforementioned draft decision to discontinue the proceedings, but relevant and reasoned objections were raised which led this Agency to reconsider its initial interpretation, reaching an agreement with the

other authorities on the assessment of the existence of an infringement on the part of GLOVOAPP, without being obliged at any time to maintain its initial position.

On the basis of the above, the present claim is rejected.

THIRD. — NULLITY OF THE ADMINISTRATIVE ACT ON THE GROUND THAT THE INFORMATION NECESSARY TO ESTABLISH AN INFRINGEMENT IS LACKING

GLOVOAPP considers that under no circumstances can their conduct be sanctioned in the form of a reprimand, for the reasons set out below.

3.1 Absence of subjective elements of the infringement. Nullity of penalty

GLOVOAPP considers that the existence of intentional or negligent action in the present case has not been analysed in order to be able to impose a penalty in the present case. In other words, the existence of the subjective element (guilt) required by Law 40/2015 in order to establish the existence of an administrative offence has not been analysed.

Stresses GLOVOAPP that it has been proven that it has never intentionally wanted to disregard the complainant's right of withdrawal. The opposite is true. It has immediately taken this right into account once it has been transferred by this Agency.

GLOVOAPP therefore states that it must be borne in mind that the AEPD should have carried out this analysis and that, therefore, it cannot be established that Glovo intended to infringe the data protection legislation (in the way that it wished to hinder, prevent or not comply with the complainant's right to erasure), and that the assessment of that intention as an essential element of the administrative offence was disregarded. GLOVOAPP takes the view that the imposition of a penalty would be null and void.

In this regard, the Agency repeats what has been stated above, to the effect that we do not consider that there would have been a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received by channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case.

On the basis of the above, the present claim is rejected.

3.2. The absence of evidence rebutting Glovo's presumption of innocence. Nullity of penalty

GLOVOAPP submits that the administration bears the burden of proving the guilt of the person concerned, which must be proved by any of the means admitted in law.

And that, in the present case, it is not apparent that there is absolutely any evidence capable of rebutting the presumption of innocence which, within the administrative and sanctioning sphere, is fully applicable to relations between the administration and those

administered, as has been recognised by countless judicial decisions in all hierarchical and territorial areas.

In the present case, GLOVOAPP takes the view that the AEPD confines itself to reviewing the background to the file in the Agreement, but in no way can it be said that we are faced with a clearly intentional infringement of data protection rules by Glovo, especially if, as has been shown in the facts, the complainant's right to erasure was clearly respected.

GLOVOAPP considers that in the present case there is no real incriminating evidence at the time of that initiation of proceedings to suggest that there is guilt in GLOVOAPP's conduct.

In this regard, the Agency stresses that it does not understand that there was a clear intention to breach the data protection rules, but considers that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received by channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case.

As regards the evidence to that effect, GLOVOAPP stated in its reply to the transfer of the complaint and in its written observations on the decision to initiate the penalty proceedings that the request to delete the complainant's personal data had not been complied with, since it had not been possible to assign it into a specific SAC agent, since it had not placed an order and had not been assigned a specific city or territory. It was this situation that led to the failure to comply with the request made. And that, after becoming aware of the complaint, GLOVOAPP took measures to prevent this type of situation from recurring in the future (which has been positively assessed and it has been decided to replace a penalty in the form of a fine for issuing a reprimand, under the terms of the GDPR).

On the basis of the above, the present claim is rejected.

3.3. Absence of guilt. Nullity of penalty

GLOVOAPP insisted that, in the specific case, at no time the data protection legislation had been omitted or infringed, GLOVOAPP considered that it had fulfilled all its obligations in a religious manner. There has been no intention to infringe, quite the contrary.

GLOVOAPP considers that it has demonstrated to the AEPD its willingness to comply with the rules on the protection of personal data by immediately deleting the complainant's data once the complaint has been forwarded by the AEPD and ensuring that users' rights are fully satisfied at all times regardless of the channel they are exercised.

For all the above arguments, GLOVOAPP considers that there is a complete absence of evidence of guilt and, consequently, a violation of the fundamental right to the presumption of innocence enshrined in the Spanish Constitution.

In this regard, the Agency stresses that it does not consider that there was a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received via channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case. It therefore considers that there is sufficient evidence to show that GLOVOAPP acted negligently, which determines the existence of that infringement.

On the basis of the above, the present claim is rejected.

3.4. Absence of the principles of criminality and presumption of innocence. Nullity of penalty

GLOVOAPP points to the importance that the legal system attaches to the principles of criminality and the presumption of innocence in the context of the administration's power to impose penalties, and the extensive acceptance in the case-law of the obligation to apply those principles to the administrative penalty procedure, which must be compared with what happened in the present proceedings.

GLOVOAPP considers that it has been duly demonstrated that it has always acted in good faith, making every effort to comply with data protection rules in the belief that it is lawful, since it is its requirement as a controller of the personal data of data subjects and with a view to never jeopardising their rights and freedoms. There is therefore no clear 'intent' in failing to comply with the legislation in force, since it took all the necessary and appropriate actions to comply with the rules and has prudently aligned its actions with the law.

In this regard, the Agency stresses that it does not consider that there was a clear intention to breach the data protection rules, but that GLOVOAPP acted negligently by failing to provide for an internal mechanism to deal with requests concerning the exercise of rights under the legislation on the protection of personal data received via channels other than those initially provided for. In particular, in cases where the system could not assign a given SAC agent, as a specific city or territory cannot be assigned to the user, as was the case in the present case. It therefore considers that there is sufficient evidence to show that GLOVOAPP acted negligently, which determines the existence of that infringement.

On the basis of the above, the present claim is rejected.

IV

Right to erasure

Article 17 '*right of erasure ('right to be forgotten')*' of the GDPR provides that:

'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 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).*

2. *Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase such data, the controller, taking account of available technology and the cost of the implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any link to, or copy or replication of, those personal data.*

3. *Paragraphs 1 and 2 shall not apply to the extend that processing is necessary:*

- (a) *for exercising the right of freedom of expression and information;*
- (b) *for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- (c) *for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) and (3);*
- (d) *for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1), in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or*
- (e) *for the establishment, exercise or defence of legal claims'.*

Article 15 ‘Right of erasure’ of the Spanish LOPDGDD provides that:

'1. The right to erasure shall be exercised in accordance with the provisions of Article 17 of Regulation (EU) 2016/679.

2. When such erasure derives from the exercise of the right to object pursuant to article 21.2 of Regulation (EU) 2016/679, the controller may preserve the necessary data subject's identification data in order to prevent future processing for direct marketing purposes.'

In the present case, it is common ground that the complainant had requested GLOVOAPP to delete his personal data on at least four occasions.

V

Modalities for the exercise of the rights of the data subject

Article 12 '*Transparent information, communication and modalities for the exercise of the rights of the data subject*' of the GDPR states that:

'1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject 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.

3. 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. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. 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.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. 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 ‘General provisions on the exercise of rights’ of the Spanish LOPDGDD provides that:

‘1. The rights established in Articles 15 to 22 of Regulation (EU) 2016/679 may be exercised directly or through a legal or voluntary representative.

2. The controller shall be obliged to inform the data subject about the means available to him or her to exercise his or her rights. Such means shall be easily accessible by the data subject. The exercise of the right may not be denied on the sole ground that the data subject chooses a different means

3. The processor may process, on behalf of the controller, any request submitted by the data subjects to exercise their rights if this is established in the binding contract or legal act.

4. The evidence of compliance with the duty to respond to the request for the exercise of rights submitted by the data subject shall be the responsibility of the controller.

5. Where the laws applicable to certain processing establish a special regime that affects the exercise of the rights provided for in Chapter III of Regulation (EU) 2016/679, the provisions of those laws shall apply.

6. In any case, the holders of the parental authority may exercise in the name and on behalf of minors under fourteen years old the rights of access, rectification, cancellation, opposition and any other rights to which they may be entitled in the context of this organic law.

7. Any actions carried out by the controller to address requests to exercise these rights shall be free of charge, notwithstanding the provisions of articles 12.5 and 15.3 of Regulation (EU) 2016/679 and paragraphs 3 and 4 of article 13 of this organic law.’

In the present case, it is common ground that the complainant requested the deletion of his account and personal data on at least four occasions. The last of these on 13 November 2019. However, it was only on 16 September 2020 that GLOVOAPP confirmed to the complainant that it duly complied with that request, after having received the transmission of the aforementioned complaint from the Agency.

Although the complainant had not used the form for that purpose, he had contacted a customer service agent via a chat and had received an automatic reply from the undertaking to reply to it within 24 hours.

Indeed, it is the responsibility of the controller to ensure the satisfaction of data subjects' rights in general and, in particular, to comply with any requirements of the GDPR in relation to these rights. The accountability principle, in line with Article 5 (2) GDPR, implies that the controller must adapt its internal processes to comply with its regulatory obligations, in line with the organisation and processing of personal data it carries out. In addition, the controller must demonstrate that the solutions adopted comply with the requirements of the regulations.

In this context, the controller can and should have mechanisms that allow for the exercise of each of the rights in a simple way for data subjects and to give them full satisfaction in the shortest possible time. The controller should also demonstrate flexibility in the interaction with the data subject on a specific application, regardless of its internal policy. The fact that the request was made by means of an alternative to the mechanisms put in place by the undertaking should not be a reason not to comply with it.

Therefore, on the basis of the evidence available, the known facts are considered to constitute an infringement, attributable to GLOVOAPP, of Article 12 GDPR, read in conjunction with Article 17 GDPR.

VI

Sanction of the infringement of Article 12 GDPR

The infringement of Article 12 of the GDPR entails the commission of the infringements referred to in Article 83 (5) of the GDPR, which, under the heading '*General conditions for the imposition of administrative fines*', provides:

'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:

(...)

(b) the data subjects' rights pursuant to Articles 12 to 22; (...)

In that regard, Article 71 ('Infringements') of the Spanish LOPDGDD provides that:

'The actions and behaviours referred to in sections 4, 5 and 6 of Regulation (EU) 2016/679, as well as those which are contrary to this organic law, shall constitute infringements.'

For the purposes of the limitation period, Article 74 'Minor infringements' of the Spanish LOPDGDD states:

'In accordance with sections 4 and 5 of article 83 of Regulation (EU) 2016/679, any infringement consisting on merely formal lack of compliance with the provisions

mentioned therein, especially the ones listed below, shall be considered a minor infringement and its limitation period shall be one year:

(...)

(c) Failing to attend to the requirements to exercise any of the rights established by articles 15 to 22 of Regulation (EU) 2016/679, unless this results from the implementation of article 7.2.k) of this organic law’.

VII Sanction for the infringement of Article 12 GDPR

Without prejudice to Article 83 of the GDPR, Article 58 (2) (b) of the GDPR provides as follows:

‘Each supervisory authority shall have all of the following corrective powers:

(...)

(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; (...’”

Recital 148 of the GDPR states:

‘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..’

In accordance with the evidence available, the infringement in question is considered to be minor for the purposes of Article 83 (2) of the GDPR, given that in the present case it was a specific case, as a result of a one-off error (of which there are no similar records in this Agency), which would have already been corrected, which makes it possible to consider a reduction in fault in the facts, and it is therefore considered to be lawful not to impose a penalty consisting of an administrative fine and to replace it by issuing a reprimand.

Therefore, in accordance with the applicable legislation and assessing the criteria for graduation of penalties established,
the Director of the Spanish Data Protection Agency DECIDES TO:

FIRST: Issue GLOVOAPP23, S.. L., with VAT B66362906, for an infringement of Article 12 of the GDPR, as set out in Article 83 (5) of the GDPR, a reprimand.

SECOND: Notify this resolution to GLOVOAPP23, S.L.

In accordance with Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

In accordance with Article 48.6 of the LOPDGDD, and in accordance with Article 123 of the LPACAP, interested parties may, by way of option, lodge an appeal against this decision with the Director of the Spanish Data Protection Agency within one month of the day following notification of this decision or direct administrative appeal to the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the Fourth Additional Provision of Law 29/1998 of 13 July on Administrative Jurisdiction, within two months of the day following notification of this act, as provided for in Article 46 (1) of that Law.

Finally, we would point out that, in accordance with Article 90.3 (a) of the LPACAP, the final administrative decision may be suspended as a precautionary measure if the interested party indicates their intention to lodge an administrative appeal. If this is the case, the interested party must formally inform the Spanish Data Protection Agency of this fact by submitting it via the Agency's electronic register [<https://sedeagpd.gob.es/sede-electronica-web/>] or through one of the other registers provided for in Article 16.4 of Law 39/2015 of 1 October. It shall also forward to the Agency the documentation proving that the administrative appeal has actually been lodged. If the Agency is not aware of the lodging of the administrative appeal within two months of the day following notification of this decision, it shall terminate the provisional suspension.

938-050522

Mar España Martí
Director of the Spanish Data Protection Agency



Procedure No: PS/00138/2022

IMI Reference: A56ID 322069- A60DD 411333- Case Register 357086

FINAL DECISION

From the procedure instructed by the Spanish Data Protection Agency and based on the following

FACTS

FIRST: On 8 August 2022, the Director of the Spanish Data Protection Agency agreed to initiate penalty proceedings against EUROPYMES SERVICIOS INTEGRALES S.L. (hereinafter, EUROPYMES) in order to impose an administrative fine of 1000 euros (one thousand euros) for the alleged infringement of article 17 GDPR.

SECOND: On 17 August 2022, EUROPYMES paid the penalty. The recognition of liability has therefore not been established.

THIRD: The payment made entails the waiver of any action or remedy in administrative means against the sanction, in relation to the facts referred to in the Agreement to initiate the present proceedings.

LEGAL GROUNDS

I Competence

In accordance with Article 58 (2) of Regulation (EU) 2016/679 of 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 free movement of these data (GDPR), and as set out in Articles 47, 48.1, 64.2, 68.1 and 68.2 of Organic Law 3/2018 of 5 December 1995 on the protection of personal data and guarantee of digital rights (hereinafter LOPDGDD) is competent to adopt this final decision the Director of the Spanish Data Protection Agency.

In addition, Article 63(2) of the LOPDGDD provides that: "*The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures*".

II Termination of the penalty proceedings by voluntary payment

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (hereinafter LPACAP), under the heading '*Termination in penalty proceedings*', provides:



“(…)

2. Where the penalty is only pecuniary in nature or it is possible to impose a pecuniary and a non-pecuniary penalty but the latter has been justified as inadmissible, the voluntary payment by the presumed offender, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the replacement of the altered situation or the determination of compensation for the damages caused by the commission of the infringement.

(...).”

According to the above, the Director of the Spanish Agency for Data Protection DECIDES:

FIRST: To declare the termination of the proceedings **PS/00138/2022**, in accordance with Article 85.2 of the LPACAP.

SECOND: To notify this decision to EUROPYMES SERVICIOS INTEGRALES S.L.

In accordance with Article 50 of the Spanish LOPDGDD, this Decision shall be made public once it has been notified to the interested parties.

Against this decision, which puts an end to the administrative procedure as required by Article 114(1)(c) of the Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations, interested parties may bring an administrative action before the Administrative Chamber of the National High Court, in accordance with the provisions of Article 25 and paragraph 5 of the fourth additional provision of Law 29/1998, of 13 July, regulating the Dispute-Administrative Court, within two months of the day following the notification of that act, as provided for in Article 46(1) of that Law.

937-240122

Mar España Martí
Director of the Spanish Data Protection Agency



Berlin Commissioner
for Data Protection
and Freedom of Information

521.14435.6

CR 191470

DD 469870

Berlin, 17.05.2023

Final Decision

Preliminary remarks

The complaint (ref. no. 521.14435) was raised before the Berlin DPA in April 2021. It was transferred to the supervisory authority Netherlands, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by [REDACTED] in accordance with Article 56 GDPR. The LSA conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA proposed a Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

Summary of the Case

1. On 28 June 2020 the complainant made a booking via the platform [REDACTED] for the accommodation [REDACTED] On [REDACTED] 29 June 2020 he received a notification from this accommodation in which they invited him to contact them at [REDACTED] After contacting the e-mail [REDACTED]

Berlin Commissioner for Data Protection
and Freedom of Information (BfBDI)

Alt-Moabit 59-61, 10555 Berlin
Germany

Phone: +49 30 13889-0
Fax: +49 30 215 50 50

Office hours: Monday to Friday from 10 am
to 3 pm, Thursday from 10 am to 6 pm

E-mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de



address he received an e-mail from another e-mail address on the same day stating that [REDACTED] had not updated the calendar for the booked accommodation, therefore his booking was not possible. After some e-mails back and forth the complainant opted for a comparable accommodation [REDACTED] and paid the requested amount to a Spanish bank account. Upon arrival the complainant had found that the accommodation did not exist and that he had been the victim of fraud.

2. The complainant suspects that there has been a data breach at [REDACTED] given that he had been contacted with precise information about his planned stay in [REDACTED]

Investigation by the NL SA

3. On 19 August 2022 the NL SA requested additional information regarding this complaint from [REDACTED] The NL SA requested [REDACTED] to clarify if the complainant had contacted [REDACTED] about his experience with the initial accommodation provider [REDACTED] The NL SA also asked [REDACTED] [REDACTED] has been identified by [REDACTED] as a fraudulent accommodation provider. On 8 September 2022 [REDACTED] replied to this request.
4. [REDACTED] replied that they found no contact between them and the complainant in relation to his concerns about the accommodation. [REDACTED] confirms that the accommodation provider was identified as fraudulent by [REDACTED] on 30 June 2020. [REDACTED] explains that in their standard procedures, this triggers a cancellation by [REDACTED] of reservations made on the platform with the accommodation provider. In relation to this specific reservation [REDACTED] systems show that the complainant had already cancelled the reservation himself. The cancellation was free, so the complainants credit card was not charged at that point by [REDACTED]. Additionally, since the payment was handled directly by [REDACTED], the accommodation provider would not have received any payment details relevant to the complainant from [REDACTED]
5. [REDACTED] informed the NL SA that the fraudulent accommodation provider has invited the data subject to reply via an email address shared by the fraudulent accommodation provider [REDACTED] states that if the complainant did respond directly to this email address and not via the [REDACTED]

platform, it is possible that the complainant may have provided personal data to the fraudulent accommodation provider directly, including potentially his credit card details. [REDACTED] clarifies that this would have taken place outside of the [REDACTED] platform and would therefore not be visible to [REDACTED]

6. The NL SA looked into the communication between the complainant and the fraudulent party, and have confirmed that the complainant emailed directly to the fraudulent party.
7. On 12 September 2022 the NL SA contacted the Berlin SA via 61VMN 436950 and shared the reply of [REDACTED] and an assessment of the case. The NL SA invited the Berlin SA to share the reply of [REDACTED] with the complainant. The NL SA believed that there was no indication of a GDPR violation and asked the Berlin SA if it was possible to contact the complainant and ask him to withdraw his complaint. On 21 November 2022 the NL SA sent a reminder to the Berlin SA via 61VMN 460002 and asked if the Berlin SA agreed with the NL SA's assessment of this complaint. The NL SA has not yet received a response from the Berlin SA.

Norm allegedly infringed

Article 32 GDPR

Proposed action by the NL SA

8. Considering the above the NL SA finds no infringement of the GDPR in this case.
9. The NL SA deems this matter investigated to the extend appropriate and rejects the complaint ex article 60(8) GDPR. The supervisory authority with which the complaint was lodged (the regulatory authority in Berlin) shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

Appeal Notice to the complainant

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the notification of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) or for the record of the

clerk of the court. Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection and Freedom of Information



Berlin Commissioner
for Data Protection
and Freedom of Information

521.15203.13

CR 69327

DD 475767

Berlin, 17.05.2023

Final Decision

Preliminary remarks

The complaint (ref. no. 521.15203) was raised before the Berlin DPA in October 2021. It was transferred to the supervisory authority Netherlands, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by [REDACTED] in accordance with Article 56 GDPR. The LSA conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA proposed a Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

Summary of the Case

1. On 11 August 2021 the representative of the complainants, [REDACTED] left a review of an accommodation on the platform of [REDACTED]
[REDACTED] On 3 September 2021 the complainant noticed that the

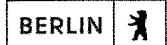
Berlin Commissioner for Data Protection
and Freedom of Information (BlnBDI)

Alt-Moabit 59-61, 10555 Berlin
Germany

Phone: +49 30 13889-0
Fax: +49 30 215 50 50

Office hours: Monday to Friday from 10 am
to 3 pm, Thursday from 10 am to 6 pm

E-mail: mailbox@datenschutz-berlin.de
Website: www.datenschutz-berlin.de



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 [REDACTED] to complain about the accommodation provider. On 4 September 2021 the accommodation provider posted an updated reply to the review which, again, contained the 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 [REDACTED]. The accommodation provider removed their reply on 6 September 2021 and posted an updated reply on 7 September 2021 in which the names of the complainants were not mentioned.

2. [REDACTED] sent an auto-reply to the representative on 4 September 2021 and another response on 1 October 2021. In this response [REDACTED] informed the representative that they have noted the complaint with the accommodation. [REDACTED] informed the representative that reviews are updated within 10 days and that she should not be able to see the review afterwards.
3. On 2 October 2021 the representative responded to the e-mail of [REDACTED] explaining that the reply of the accommodation partner has changed multiple times in the meantime and that she does not understand what [REDACTED] 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 is that she was concerned that the monitoring mechanism used by [REDACTED] 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.
4. On 2 October 2021 the representative filed a complaint at the Berliner Beaufragte für Datenschutz und Informationsfreiheit (hereinafter: Berlin SA) on behalf of the complainants. The complainants believe that there is an systematic failure with regard

to the publication of names of data subjects in the reviews on the platform of [REDACTED]

5. On 31 January 2022 the complaint was transferred to the NL SA.

Investigation by the NL SA

6. On 19 August 2022 the NL SA requested additional information regarding this complaint from [REDACTED]. The NL SA asked [REDACTED] to verify that they check the reviews on their platform for names of data subjects and how they monitor the reviews. On 8 September 2022 [REDACTED] responded to this request.
7. [REDACTED] 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 [REDACTED] Content Moderation 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 [REDACTED] Content Moderation Team.
8. In this specific case, the response was published while certain names were still visible. When this happens, [REDACTED] standard process is to promptly delete such posts when they are flagged, e.g. when a customer sends a related message to [REDACTED] 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 [REDACTED] platform from 12 August 2021 until 6 September 2021. This means that the data subject's personal data in the accommodation provider's response were removed within 3 days after the data subject updated her review to complain about it.
9. On 12 September 2022 the NL SA shared [REDACTED] response with the Berlin SA. In this VMN the NL SA indicated that the information provided by the complainant and

[REDACTED] proves that the content moderating system is not flawless, but in our opinion, this does not indicate that the measures taken by [REDACTED] 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 [REDACTED] will delete the posts. Further investigation would be required to gain a deeper understanding of the content moderating system and the exact steps and parameters.

10. The NL SA finds such an investigation disproportionate with regard to this specific complaint, considering that the personal data of the complainant were removed within 3 days after the representative updated her review to complain about it.
11. On 12 September 2022, the NL SA invited the Berlin SA to share the reply of [REDACTED] with the complainant and to provide their feedback concerning the handling of this complaint. On 21 November 2022 the NL SA sent a reminder to the Berlin SA. The NL SA did not receive a response from the Berlin SA.

Norm allegedly infringed

Articles 5, 6, 7, 12, 13, 14 and 17 GDPR.

Proposed action by the NL SA

12. Considering the above the NL SA finds no infringement of the GDPR in this case.
13. The NL SA deems this matter investigated to the extend appropriate and rejects the complaint ex Article 60(8) GDPR. The supervisory authority with which the complaint was lodged (the regulatory authority in Berlin) shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

Appeal Notice to the complainant

Against this decision a lawsuit before the Verwaltungsgericht Berlin (administrative court of Berlin), Kirchstraße 7, 10557 Berlin is admissible. The lawsuit needs to be filed in written form within one month after the notification of this decision, it can also be filed as an electronic document with a qualified electronic signature (QES) or for the record of the clerk of the court.

Please, note that in case of filing the lawsuit in writing the legal deadline is only met if the lawsuit reaches the administrative court within the deadline.

The Berlin Commissioner for Data Protection and Freedom of Information



Record no. 8492/163/20

IMI Case no. 380803.1

9 December 2022

Final Decision of the Deputy Data Protection Ombudsman

Matter Processing of health information by the employer, accuracy of personal data, informing the data subjects, disclosure of personal data to the police, user log data and the data subject's right of access to data

Complainant [REDACTED]

Controller [REDACTED]

Complainant's claims and their justification

1. On 26 October 2020, the complainant instituted a case with the Office of the Data Protection Ombudsman concerning the processing of personal data by a controller. The complainant alleged that [REDACTED] had maintained an extensive data file containing health information on its employees. It was alleged that this data file included the times of absence due to illness and the employees' diagnoses. The complainant has alleged that her data was stored in this file for 20 years. According to the complainant, she was dismissed in 2017, but the above-mentioned information on her was allegedly still stored until at least 2020. The complainant has also alleged that her data in the file was also partly inaccurate. Furthermore, the complainant has alleged that this data was used against her when she contested her dismissal.
2. According to the complainant, she has asked [REDACTED] for access to her personal data. In addition, the complainant said that she has requested access to the log data related to the data file in question. The complainant has not been given access to the log data. The complainant was given a number of justifications for why the employer considered that it had the right to store the data. Information on the diagnose listing included in the data file had not been given to the complainant. The complainant eventually obtained the information by other means.
3. The document instituting the case also makes other allegations, including that the health information was stored in a system called MAPS, which is used by all vessels sailing under the Finnish flag. Furthermore, it has been alleged that any nurse working on any vessel would have access to the data of any shipboard employee, regardless of the vessel on which the nurse is working.

Information provided by the controller

The request made by the complainant to the controller



4. The complainant has requested access to the data on at least 10 January 2020 and 3 February 2020. Among other documents, the complainant has delivered the reply given by the controller to her request on 1 April 2020 to the Office of the Data Protection Ombudsman.
5. The reply states that the complainant asked for a copy of her sick leave certificates for 2001–2017. The controller has stated that it is in possession of the complainant's sick leave certificates for 2017 and a single sick leave certificate from 2016. The controller has promised to deliver these copies to the complainant. The controller has also stated that it is in possession of the material related to the trials.
6. Furthermore, the reply states that the disclosure of log data is provided for in the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare. The controller has stated that the Act only applies to the electronic processing of social welfare and health care client data. According to [REDACTED], it is not a social welfare or health care service provider as referred to in this Act. Therefore, [REDACTED] considers that it does not have a statutory right or obligation to deliver log data from electronic systems to the complainant.
7. According to the controller, the complainant's request asked the controller to state the basis on which her data was processed in police interviews. In this regard, [REDACTED] has referred to Article 9(2)(f) of the General Data Protection Regulation (GDPR).
8. According to the controller, the complainant also enquired why a nurse working for [REDACTED] had disclosed information on forthcoming occupational health discussions to certain employees in the organisation. The controller stated that the question involved email messages related to the occupational health discussions and scheduling a time for the discussion. In this regard, [REDACTED] has stated that the employer has the right to process an employee's personal data when the processing is necessary for complying with the obligations and special rights of the controller or data subject in the field of employment legislation. Furthermore, the controller stated that an employee's personal data may also be processed for the purpose of assessing their ability to work. The data was only processed by individuals who required the data for performing their duties. Furthermore, the controller stated that access to employees' health information is restricted to individuals tasked with preparing, making or implementing decisions affecting employees.
9. According to the controller, it keeps sick leave certificates for as long as they are required by the rights and obligations related to employment contracts. According to the reply issued by the controller, the data is erased when no longer required. According to the reply, [REDACTED] is not in possession of the complainant's sick leave certificate copies for a period of 17 years. The controller stated that it has collected the complainant's data from the employer's electronic system in which the information on the employee's sick leave periods has been saved. The reply again refers to points (b), (f) and (h) of Article 9(2) of the GDPR.

Office of the Data Protection Ombudsman's request for information



10. The Office of the Data Protection Ombudsman has asked the controller for information on this matter. The controller replied to the request on 31 January 2022.

[REDACTED]'s data files containing employee health information

11. The information provided by [REDACTED] confirms that it has maintained two data files intended for internal use (the MAPS human resources management system and Medakt patient record system), which have contained employees' health information, among other things.

12. [REDACTED] has said that MAPS is its HR management system used to manage employment contracts and fulfil the employer's obligations, such as salary payment.

13. Medak, on the other hand, is said to be an electronic patient record system used on [REDACTED]'s vessels, into which the nurses licensed by the National Supervisory Authority for Welfare and Health (Valvira) and working on board record the procedures performed on patients and the medicines administered to them, as required under section 12, subsection 1 of the Act on the Status and Rights of Patients (785/1992). Patients can include both passengers and crew members who have fallen ill during the voyage. Employee health information is recorded in the Medakt patient record system if the employee falls ill while on board the vessel and cannot use onshore occupational health care services.

Data content of the data files used by [REDACTED]

14. The MAPS system contains the personal data of approximately 6,000 data subjects. Some of these data subjects are current employees of [REDACTED] and some are former employees. All vessels considered, the Medakt system contained the personal data of approximately 19,350 patients (5,600 employees and 13,750 passengers) at the beginning of 2022.

15. Employment-related information, such as the names and contact details of employees, employment contract status, qualifications, completed training, as well as information concerning salary payment and health care costs, have been stored in the MAPS system. According to chapter 2, section 12 of the Seafarers' Employment Contracts Act (756/2011), the employer has an obligation to pay for the treatment of sick employees and compensate them for the travel costs of getting home from the vessel.

16. The MAPS system has also contained employee absence data, including data on absences due to illness with dates and ICD diagnosis codes, which are used to determine whether the employee is entitled to pay during their absence. [REDACTED] further stated that not all absences are paid, which is why the employer needs to process data on the reasons for absences due to illness to a certain extent in order to ensure accurate salary payment. In addition to the codes, the diagnoses have been recorded in the system in plain text. However, according to the information provided by the controller, both ICD and plain-text diagnoses were erased from the system in 2018–2019. The system no longer contains such information. At present, only the information that an employee has been absent due to an illness and



whether the absence was paid or unpaid or, for example, family leave, is recorded in the system. [REDACTED] has assessed that, taking into account the purpose of the system, it is not necessary to record diagnoses in it.

17. The controller has stated the processing described above is based on the provisions of Article 6(1), points (c) and (f) of the GDPR (controller's legal obligation and controller's legitimate interest). The employer's statutory obligations, such as salary payment during illness, are said to be based on either the Seafarers' Employment Contracts Act or the Employment Contracts Act, depending on the employee's position.
18. The employees' dates of birth, names and addresses, as well as employment information such as vessel and rank, have been saved in the Medakt system. According to the information given, personal profiles are not created in the system for passengers as they are for employees. The identifying information of passengers, such as the name and date of birth, are instead saved in a text typed in connection with each appointment. Information on the cause and time of treatment, procedures performed and medicines dispensed from the ship pharmacy are also recorded in the system. According to the information provided, only nurses working on board the vessel make entries in the Medakt system, and only they have access to these entries.
19. The controller has stated that health information is processed by virtue of Article 9(2)(h) and Article 9(3) of the GDPR. Furthermore, the controller's reply also referred to section 6, subsection 1, paragraph 4 of the Data Protection Act (1050/2018), according to which Article 9(1) of the General Data Protection Regulation does not apply when a healthcare service provider in the course of arranging or providing services processes data it has received in the context of these activities on the state of health or disability of the person or on the healthcare and rehabilitation services received by a person, or other data necessary for the treatment of the data subject. The controller has also referred to the legislative materials of the Data Protection Act. According to the controller, the legislative materials state that "service provider" is a general concept that covers both the organiser and provider of a service. According to the controller, these include health care and social welfare units and professionals as well as auxiliary personnel working under them. Therefore, the nurses working on ships are said to process health information by virtue of the derogation referred to above.
20. The reply also refers to the Act on Ships' Medical Stores (584/2015). According to the controller, crew health care and the obligation to record the procedures performed are based on the above-mentioned enactment. The purpose of the Act on Ships' Medical Stores is to ensure that members of a ship's crew have the possibility to receive appropriate first aid and medical care on board the vessel in case of illness or injury. According to section 9 of the Act, vessels of certain categories must have a medical journal regarding the operation of their medical store, in which the relevant personnel shall enter all acquisitions made to the medical store, any drugs dispensed to patients and all performed procedures, as well as drugs and medical supplies removed from the medical store. All personal data must be stored separately from the information regarding drugs and medical supplies. All medical journal entries shall be made in the working language of the



ship. The medical journal must be kept in such a way that the entered data remains intact and unchanged. The medical journal must be preserved for at least five years after the last entry. The medical journal must be kept with the ship's medical store. The provisions on the secrecy of patient record information laid down in the Act on the Status and Rights of Patients (785/1992) are applied to the secrecy of all information entered into the medical journal.

[REDACTED]'s operations and section 5 of the Act on the Protection of Privacy in Working Life (759/2004)

21. According to its reply to the request for information, the controller has processed employees' health information for the payment of sick pay or comparable benefits linked to the employee's health. When an employee has fallen ill while working on a ship, the ship's nurse has recorded this in the Medakt patient record system. If the illness led to sick leave, this was recorded in the MAPS system after the employee had delivered the sick leave certificate. Furthermore, the controller stated that the nurses serve as part of HR administration when accepting the employees' sick leave certificates. The employees can deliver the sick leave certificate to the ship's nurse or an onshore HR representative.
22. According to the information provided by [REDACTED], health information has only been processed by its employees tasked with preparing, making or implementing employment-related decisions based on such information. The controller has stated that such personnel is limited to two HR secretaries. The employer has specifically designated the processing of health information as part of these employees' duties. These individuals are under an obligation of secrecy both during and after their employment.
23. According to [REDACTED], it has stored employee health information saved into the MAPS system so that personnel such as payroll clerks have not had access to diagnoses or ICD codes. Payroll clerks have only had access to information on whether the absence was paid or not. The controller has also stated that it has erased unnecessary health information from the data file as required by section 5 of the Act on the Protection of Privacy in Working Life.
24. With regard to the Medakt system, [REDACTED] has stated that it has not processed the data saved into the system at all as an employer. According to [REDACTED], only the nurses working on ships have access to the system. The data stored in the system has not been disclosed to [REDACTED]'s HR administration, and HR employees do not have access to the system.

Access rights to the data files in question

25. According to the reply to the request for information, HR administration employees whose duties include the processing of data contained in the MAPS system have access to the system. Access rights have been restricted so that employees only have access to data required for the performance of their duties. The part of the system used by the HR administration has access to all data stored in the system but, according to the information provided by the controller, access to this data is



also restricted according to the needs of HR employees. The MAPS Sjölöner system is also used by ship's nurses.

26. MAPS Omborddata, on the other hand, is described as being used on board the company's vessels. Employees who use the system can only access the data of crew members working on the ship in question. Employees have limited access to this data. Supervisors do not have access to all information on their subordinates.
27. In addition to the above, ship's nurses have recorded sick leave and diagnosis information in the MAPS system if the employee fell ill while working on board or delivered their sick leave certificate to HR administration through the ship's nurse.
28. Nurses working on ships and performing duties arising from the Act on Ships' Medical Stores and the Act on the Status and Rights of Patients have had access to the Medakt system. According to the information provided by the controller, no other persons have had access to the system. The Medakt system is not connected to other patient information systems, such as the Kanta service. In other words, information is not conveyed to other health care operators from the Medakt system.
29. As a rule, every employee has their own profile in the Medakt system according to the information provided by the controller. Substitute health care workers on ships use Medakt with a ship-specific user ID. Substitutes have been instructed to sign their entries with their own names. However, the identity of an entry's author can also be determined later from the shift lists.
30. According to the information provided, ship's nurses have had access to the Medakt data of any [REDACTED] vessel since, like other crew members, nurses can work on different ships. The same nurse is not always on duty, so another nurse may have a justified need to continue a task started by a different nurse and use the data stored in the system to complete the task. However, nurses are only permitted to process data necessary for the patient's care. Only the administrators have rights to make changes in the system. Nurses are not administrators.

Informing the data subjects

31. The controller has stated that the matter at hand has shown that employees have not been sufficiently informed of the processing discussed herein. According to the reply to the request for information, this deficiency will be rectified as soon as possible. [REDACTED] will inform the data subjects as required by the GDPR.

Storage of data

32. According to the information provided, information on sick leaves and the right to pay is stored in the MAPS system for ten years from the end of the absence. Older sick leave and pay entitlement information has been erased. According to [REDACTED], all ICD codes and diagnoses have been erased from the MAPS system in 2018 and 2019, and such information is no longer being saved into the system. [REDACTED] is in the process of deploying a new system. The data storage periods will be revised in connection with the deployment.



33. At the moment, the data in the Medakt system is being stored for an indefinite period. According to the information provided, the health information is saved because it has been considered necessary for monitoring the employees' health. Information on an employee's injuries or health problems can be needed later, for example for the processing of insurance cases or occupational disease surveys. The Medakt system contains information from 2012 onwards. The storage periods will be reassessed in 2022.

Accuracy of the data recorded in the file

34. Data subjects have had the right to review data saved in the MAPS and Medakt systems. The data has also been updated when necessary. The nurses making entries in the Medakt system have been responsible for the accuracy of their entries.

Securing the data files

35. [REDACTED]'s internal network is protected with safeguards such as a firewall and passwords. Shipboard users log into the MAPS system with task-specific usernames and passwords. Working hours are logged with personal usernames and passwords. HR administration employees have personal usernames and passwords to the MAPS system. As described above, access rights have been restricted to the information needed by employees in the performance of their duties. Only changes saved into the system are stored in the log of the MAPS system. The identity of the author of the original entry is not saved into the log.

36. The Medakt system can only be accessed from the nurse's work computer in the medical cabin. The login process has three stages. In the first stage, the nurse has to log into the Citrix service with their personal username and password. In the second stage, a one-time password is sent to the nurse by email. The Medakt system can then be launched through Citrix. After that, the user still needs to enter their personal username and password to log into the Medakt system. It has also been established that the nurses are aware that they only have the right to access the records of patients who they are actually treating. The system is not connected to any other health care information systems.

The entries involving the complainant

37. During the investigation of this matter, it turned out that it was not possible to save all ICD codes into the MAPS system in 2001. In other words, only a portion of the codes was used. It has thus been possible that absences due to illness may have been saved into the system with different codes than those in the actual diagnosis based on which the sick leave was granted. It is said that the system's users have sought to determine the closest corresponding code that could be entered into the system. In this regard, [REDACTED] has admitted that the system has been problematic in terms of data protection. The system has since been modified in this regard.



38. The complainant has alleged that the ICD code entered into the MAPS system for an absence due to illness granted in 2016–2017 does not correspond to the code on the sick leave certificate. In this regard, the controller has referred to the request for information addressed to the controller by the complainant on 3 February 2020, which was delivered with four enclosed sick leave certificates for the period in question. The controller has stated that the absence due to illness began with one code, which was later changed to a different one. According to the information provided by [REDACTED], it does not, as a rule, change codes retrospectively. In this case it is nevertheless possible that the code was changed, for example at the complainant's request, to correspond to the code of the new period of sick leave. The ICD code saved into the MAPS system corresponds to three of the four codes on the sick leave certificate delivered to [REDACTED]. [REDACTED] has stressed that the nurses can also make entries into the system on the request of employees.
39. Furthermore, the reply to the request for information emphasises that [REDACTED] [REDACTED] has had no interest, either as a controller or an employer, to modify the entries in the data file retrospectively unless prompted to do so by the data subject. [REDACTED] has also stressed that it does not record diagnoses in the system at all any more.
40. In addition, the controller has stated that signed entries saved into the Medakt system can only be edited immediately after saving. Edited entries are marked with a special symbol. All earlier versions of the entry will remain visible regardless of the edit and cannot be erased from the Medakt system. Entries made by another person cannot be edited at all, nor can entries made in the past. The date and time of an entry can be changed, but the actual time stamp will also remain visible regardless of the change.

Use and disclosure of data in the file

41. The data recorded in the MAPS system has been used for HR management, such as salary payment and the verification of its accuracy. As described above, the Medakt system is an electronic patient record system used on [REDACTED]'s vessels. According to the information provided, data from the files has not been used for purposes other than the original purpose of processing.
42. Regardless of the above, [REDACTED] has stated that the complainant's health information has been disclosed to the police for the investigation of a criminal matter. According to [REDACTED]'s response, this was not a correct course of action. The controller continued by stating that, in a pre-trial investigation, a physician or other health professional can be obliged to testify on secret patient information, for example in case of an offence for which the maximum sentence is at least six years of imprisonment. However, the criminal matter referred to herein did not involve such an offence. The controller continues by stating that the information should not have been disclosed for the criminal investigation without the patient's specific written consent.

The complainant's right of access to data



-
43. According to the information provided by [REDACTED], the information on the complainant's sick leave certificates was given to the complainant insofar as it was available. The oldest information had already been erased.
44. The response to the request for information referred to the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) repealed on 1 November 2021. According to section 18 of the said Act, a client has, for the purposes of determining or exercising the client's rights related to the processing of their client information, the right to be informed by the social welfare or health care service provider of who has used or received information concerning the client, as well as the basis for such use or disclosure. Such information shall be based on log register data and provided free of charge and without delay upon written request.
45. The controller has proposed that the obligation to disclose log data would apply to health care service providers, meaning health care units referred to in section 2, subsection 1, paragraph 4 of the Act on the Status and Rights of Patients, employers referred to in section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), as well as self-employed health care professionals. The medical care of ship crews, including on the vessels of [REDACTED], is based on the Act on Ships' Medical Stores. The obligation to record procedures performed on patients is also based on the aforementioned Act. Since the Act on the Status and Rights of Patients does not refer to the Act on Ships' Medical Stores, [REDACTED] has interpreted the provision on the disclosure of log data to mean that it is not a health care service provider as referred to in the Act and has thus considered that it does not have the right to disclose log data. In addition, [REDACTED] has stated that the log data concern the users of information systems and cannot thus be disclosed to the subject of processing by virtue of the GDPR alone. Finally, the controller has stated that it has contacted the National Supervisory Authority for Welfare and Health (Valvira) on several occasions to obtain confirmation for its interpretation. According to the information provided by the controller, however, it has not received a reply from Valvira.

Past and future measures

46. According to the information provided by [REDACTED], it is in the process of deploying a new HR information system, which will be better equipped to meet the requirements of data protection legislation than the old MAPS system. Data protection by design will be emphasised in the new system, for example by limiting storage times, improving the logging of processing data, and by requiring the secure processing of personal data. As the coronavirus pandemic has been especially hard on the tourism industry, including the business operations of [REDACTED], the development and deployment of this HR system has been delayed.
47. [REDACTED] has updated the data protection competence of its HR administration personnel through data protection training in 2020 and 2021. The company will continue investing in data protection training in the future as well. It will conduct a meticulous review of its HR data files in 2022. The purpose of this review is to ensure that the data files do not contain any old or unnecessary



information. The company's privacy statements and the data protection section in its intranet will be updated in this connection. Personnel will also be informed of the processing of their personal data before the end of 2022.

Applicant's response

48. [REDACTED]'s response was delivered to the complainant. After receiving the response, the complainant submitted a brief response to the controller and the Office of the Data Protection Ombudsman. In this email sent on 9 February 2022, the complainant alleged that the response issued by [REDACTED] contained several inaccuracies. The complainant stressed that she had addressed her request to access her data, sent on 10 January 2020, to a specifically named [REDACTED] [REDACTED] employee since, according to the complainant, this named person had disclosed the complainant's diagnoses saved into the MAPS system to the police from a period of 17 years. The complainant has likewise stressed that this specific person had not been designated as an official processor of health information by the shipping company. According to the complainant, it is unclear how this specific person had gained access to this data. The complainant stated that this person had not given the information to the complainant.
49. The complainant has referred to [REDACTED]'s response, which stated that the ICD codes and diagnoses saved into the MAPS system had been erased from the system in 2018–2019. This is not true according to the complainant. The complainant has said that she has received written information on her diagnoses in 2020 and is able to prove it.
50. According to the complainant, the claim that the data would only have been stored in the MAPS system for ten years is also incorrect. The complainant has referred to a copy of her diagnoses recorded in the MAPS system, given to her in 2020. She has also delivered this copy to the Office of the Data Protection Ombudsman. The copy shows that the first diagnosis recorded for the complainant dates to 1997. According to the complainant, the data has thus not been erased every ten years.

Supplement to response

51. [REDACTED] has supplemented its response on 10 February 2022. According to the supplement, the wrong year had been left in the response. The data was erased from the MAPS system in 2020, i.e. not in 2018–2019.

Applicant's response

52. The applicant was provided an opportunity to issue a response in the matter. The applicant issued her response proper on 22 February 2022.
53. The response claims that [REDACTED] has maintained an excessively comprehensive health information data file and neglected to inform the data subjects of the processing. In the complainant's opinion, the recording of diagnoses was illegal. Furthermore, data has been disclosed to third parties without a legal basis.



Data content of the data files used by [REDACTED]

54. As her opinion, the complainant has stated that the Medakt system is a patient information system to which the Act on Ships' Medical Stores only applies to a limited extent. The complainant has stated that only the ship's nurses and HR secretaries at the head office have access to the diagnoses. Furthermore, the complainant has expressed the opinion that a HR secretary should only have access to paper copies of medical certificates. If a nurse has both entered the diagnosis and specified whether the sick leave is paid or unpaid in the MAPS system, HR secretaries should have no reason to access the MAPS entries according to the complainant.
55. The complainant has also stated that the entries made into the Medakt system are not limited to cases of illness on board ships, but information such as the details of telephone conversations between the nurse and onshore employees is also entered into the system. Furthermore, according to the complainant, the names of prescription drugs prescribed by any physician on shore and the purchase price of the drugs are also entered into the system. According to the complainant, the shipping company normally compensates its employees for the purchase of such drugs. Compensation for medicines can be obtained for 112 days per illness, after which the employee is liable for their own medicine costs. The drug entries are no longer made after the above-mentioned time.
56. Employees are compensated for the purchase prices of prescription drugs against the receipt. The nurse delivers the receipt given by the employee to the HR secretary. The complainant has suggested that the HR secretaries can misuse the information obtained from the receipts and medical certificates. That is why, according to the complainant, some employees do not exercise their right to compensation for medicines.
57. According to the complainant, the entries made by nurses into the Medakt system normally include the nurse's name and the vessel on which the appointment took place. The complainant has suggested that even these entries are not always accurate. Entries have been known to be made for the wrong ship. At times, the name of the ship is missing from the entry altogether. According to the complainant, it is thus unclear which ship's medical store has been used. If an entry has been made for the wrong ship, that means that the medicine stocks of ships' medical stores cannot be in compliance with the Act on Ships' Medical Stores and/or ship-specific according to the complainant. The complainant states that this prevents keeping stock of medicines dispensed from ships' medical stores. Furthermore, the complainant has alleged that not all entries are related to the provisions of the Act on Ships' Medical Stores, but some of them involve health care on a more general level, such as discussions on work stress or workplace bullying (early intervention model).
58. The complainant has called into question [REDACTED]'s claim that only ship's nurses have access to the Medakt system. According to the complainant, the system also contains entries made by the representatives of private service providers (such as chiropractors / occupational health physicians who have occasionally visited the ship in port). According to the complainant, such individuals



have access to the information of many employees. The complainant has therefore stated as her opinion that the Act on Ships' Medical Stores does not apply to Medakt entries with regard to granting access to log data. According to the complainant, the system involves more than just offshore procedures or medicines dispensed from the ship's medical store.

[REDACTED]'s operations and section 5 of the Act on the Protection of Privacy in Working Life (759/2004)

59. The complainant has suggested that employees have only been instructed to deliver their sick leave certificates to the nurses and not to HR representatives. The nurse records the diagnosis into the MAPS system and sends the sick leave certificate to the designated person in HR administration. The complainant continued by stating that the employer has the right to make a copy of this original paper sick leave certificate, keep it apart from other personal data and destroy it as unnecessary in five years at the latest.

Access rights to the data files in question

60. The complainant has suggested that no payroll clerk or head of function has the right to access information on medical diagnoses. Such information is not used in payroll accounting. The nurse makes the necessary entries into the MAPS system.

Data entered into the data files

61. The complainant has alleged that the 60-day sick leave rules is being misused in the MAPS system. According to the complainant, if an employee is on sick leave for their ten-day work period, healthy for the following ten-day period and again ill for their next ten-day work period, [REDACTED] considers that the employee has also been ill during their free time, even if there is no sick leave certificate for this period of free time. The complainant has alleged that such interpretations have also been applied to situations in which an employee has been on sick leave before their annual holiday and again immediately after their holiday. The complainant suspects that, in such situations, the Finnish Social Insurance Institution (KELA) has not been notified that the employee was well between their sick leaves, with the result that the shipping company has probably also received unjustified compensations from KELA according to the complainant.

62. The complainant has stated that, by acting as described above, the shipping company is able to accumulate 60 days of sick leave as soon as possible, therefore also avoiding a new nine-day qualifying period for further compensations.

63. The complainant has alleged that the Medakt system's administrator is one of the ship's nurses. According to the complainant, this means that it has been possible to edit and erase entries. The complainant has also alleged that every nurse has been able to edit the diagnoses recorded in the MAPS system at any time and in any way.

Informing the data subjects



-
64. According to the complainant, the employees have not been informed of the extensive data files described herein, so the employees have not been able to, for example, check or request the correction of their data either. No information or instructions related to the controller's processing of its employees' personal data has been available on the company intranet.
65. According to the complainant, the nurses have been unsure of what to do when an employee has requested access to their data. According to the HR manager, such requests should be addressed to the HR manager. The complainant has called this into question, since the HR manager does not have access to data files containing health information. The complainant continued by stating that an employee may not want a certain named employee to even know that they have visited a nurse. In this connection, the complainant referred to the Act on the Status and Rights of Patients, claiming that information about such appointments is not intended for this specific individual. According to the complainant, this person has not been designated as a processor of health information.

Storage of data

66. The complainant again stressed that the claimed ten-year storage period is not true. According to the complainant, data has verifiably been stored for over 20 years. The complainant's diagnose list was printed out on 6 February 2020 and contained information on diagnoses from 1997. The complainant has said that an ex-employee had asked a ship's nurse for their data stored in the MAPS system on 10 February 2022. The nurse delivered the information to this employee on the same day. The data contained information on this person's sick leaves for the period 1990–2013. This person had not worked for the shipping company since 2013, but information on their sick leave was still being stored in the data file. At that time, the data had been stored for 32 years. According to the complainant, such storage can hardly have a purpose related to the payment of salary and benefits.

The entries involving the complainant

67. The complainant has stated that she has never requested that her diagnosis information be changed.

Use and disclosure of data in the file

68. The complainant has alleged that data in both the Medakt and MAPS systems have been used for purposes other than the purpose for which it was originally collected. According to the complainant, data has been obtained by subterfuge and disclosed to third parties, among other things. As an example, the complainant has stated the judgment of the Labour Court in matter R 24/18, issued on 19 December 2019. According to the complainant, the matter was about an employee's health information from 2006 being used against the employee in the Labour Court in 2019. The employee's employment contract had ended in 2006, continued in 2013 and ended again in 2016. According to the complainant, this proves that [REDACTED] stores quite extensive data on its former employees and, when necessary, also uses such data against the employees later.



69. According to the complainant, a certain nurse on the M/S Amorella named by the complainant violated their secrecy obligation in 2017 and disclosed the complainant's health information to a HR manager named by the complainant and to the controller's lawyer and chief operating officer; the same trio that eventually dismissed the complainant.

The complainant's right of access to data

70. Since the diagnoses had not been erased in 2018–2019, they could have been delivered to the complainant in response to her request made on 10 January 2020. The complainant only received information about her sick leave certificates for 2016–2017.

71. In this connection, the complainant has referred to the Act on Ships' Medical Stores and noted that the Act is principally related to medicines. Nurses licensed by the National Supervisory Authority for Welfare and Health hold appointments at the ship's medical store. These nurses are required to comply with the Act on the Status and Rights of Patients. Not all visits to a nurse are related to medicines, and not all entries are related to the sea voyage.

Conclusion

72. According to the complainant, she has also worked on the [REDACTED], which sails under the Estonian flag.

Hearing

73. On 29 August 2022, [REDACTED] was provided with an opportunity to express an opinion on the matter and to submit an explanation of claims and of evidence which may influence the decision, as referred to in section 34 of the Administrative Procedure Act (434/2003). At the same time, [REDACTED] was provided with an opportunity to raise considerations referred to in Article 83(2) of the GDPR that should, in its opinion, be taken into account in the decision. [REDACTED] issued its response on 13 September 2022.

74. The response issued for the hearing noted that it does not address claims based on other legislation than the GDPR.

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

75. The response issued claimed that, in the matter at hand, the personal data was not used for the supervision or assessment of the data subjects, nor were negative decisions affecting the data subjects made based on the data. Furthermore, the response claimed that health information was collected for salary payment during sick leave, and data has not been used for other purposes or disclosed to third parties without justification. Therefore, [REDACTED] maintains that the purpose of the data processing was in line with the original purpose for which the



personal data was collected and with the controller's role as employer. According to the response issued, the data has never been used for other purposes.

76. Furthermore, the response maintains that the system has only been used on ships sailing under the Finnish flag, and that the system has only been used to store the data of individuals employed by [REDACTED]. [REDACTED] has thus considered that the processing under review has not been geographically extensive, even though the company operates in the territories of several states due to its passenger ship operations.
77. Furthermore, it is maintained that, with regard to the diagnoses, the response to the complainant's request to access her data and the challenges in complying with the deadline only involved this individual complainant and did not reflect the company's general practices.
78. The response stressed that the processing referred to in the matter at hand did not give rise to discrimination against the data subjects, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation or any other significant economic or social disadvantage to the data subjects. It has been specifically stated that a matter indirectly related to the matter now instituted by the complainant has also been heard in court and, according to the response issued, the court found [REDACTED] not guilty of discrimination.

The intentional or negligent character of the infringement

79. The infringement concerning the processing of personal data assessed herein, especially with regard to the personal data processed in the MAPS system, cannot be considered intentional according to the response, as the response maintains that intentionality requires the knowing and intentional infringement of the GDPR as well as heedlessness of the obligations imposed by legislation. According to the response issued, the matter at hand has involved none of the above, nor has [REDACTED] sought to achieve financial or other advantages over its competitors in this regard. Furthermore, it has been maintained that [REDACTED] has not actively and knowingly decided to, for example, store inaccurate personal data in a personnel data file. According to the response, the company also sought to respond to the request for information as promptly as possible.
80. According to the response, the situation was rather equivalent to human error, as a result of which the system containing the personal data had not been updated to correspond to legislative storage requirements with regard to its content and storage times. The controlled was not aware of the retention of old data and its possible inaccuracy until pointed out by the complainant. When [REDACTED] became aware of this state of affairs, it began looking into the matter and changed its practices.

Action taken by the controller or processor to mitigate the damage suffered by data subjects



81. When [REDACTED] had become aware that the health information of its employees had been retained for too long and the data file may also have contained inaccurate data, it reassessed the necessity of the data processed by the company and erased data that was not necessary with regard to the employment relationship. The company conducted an overall assessment of the matter and changed its practices with regard to all employees, not just the data subject who filed the complaint.
82. In addition, the response stressed that the implementation of the complainant's request to access her data was delayed because the company sought to deliver the data containing health information, which the complainant had specifically asked for, to the complainant as securely as possible by email. However, for various reasons due to the complainant herself, the complainant had not registered herself in the service that could have been used to verify her identity. The purpose of this authentication procedure was to avoid the unlawful disclosure of health information to a third party. The complainant and [REDACTED] had engaged in protracted email correspondence before the disclosure of the data (5 March 2020: [REDACTED] receives the complainant's request to exercise her right of access; 5 March 2020: [REDACTED] sends a link to the complainant's email address via an authentication service, which the complainant can use to identify herself and confirm her contact details with her online banking codes; 5 March 2020: the complainant notifies [REDACTED]'s representative that she cannot find the link sent; 9 March 2020: [REDACTED]'s replies to the complainant, indicating the name of the sender contained in the email; 9 March 2020: the complainant asks for the link to be resent; 25 March 2020: the complainant again asks for the link to be resent; and 26 March 2020: [REDACTED] resends the link to the authentication service to the complainant's email address). In other words, [REDACTED] had sought to deliver the information requested by the complainant to her in a secure manner via encrypted email. The information could certainly have been delivered quicker but, according to [REDACTED], that would have required compromising on data security, which the company did not consider to be an option according to its response.
83. [REDACTED] considers that it has done its best to comply with the deadline provided for in Article 12(3) of the GDPR and, therefore, also the provisions of Article 15(1) of the GDPR. [REDACTED] has admitted to an error regarding the data in the file for the year 1997, because it had not delivered this data to the complainant.
84. [REDACTED] also considers that it has actively sought to resolve the matter at hand in cooperation with various authorities, such as the Data Protection Ombudsman, the police and Valvira.

The degree of responsibility of the processor or controller taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32

85. According to its response, [REDACTED] has sought to take into account the requirement of data protection by design and by default, provided for in Article 25 of the GDPR, as well as the appropriate technical and organisational measures



required by Article 32, in order to process the personal data as securely as possible. Access to the personal data in question has been restricted to individuals with duties directly related to the data and for the performance of whose duties the data is necessary. The processing of employees' health information has been restricted as referred to in section 5 of the Data Protection Act, i.e. access rights management has been used to ensure that the data is only processed by individuals entitled to do so. Other individuals have not been granted access rights to the systems in question. Also according to the response, the principle of integrity and confidentiality has been implemented by logging events in the information systems, for example. The measures safeguarding the systems against external misuse have also been bolstered.

Any relevant previous infringements by the controller or processor

86. According to its response, ██████████ has not been guilty of any relevant previous infringements, nor have the data protection authorities taken any measures referred to in Article 58(2) against it.

The degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement

87. Also according to its response, ██████████ has both sought to resolve the matter with the authority and promoted the deployment of a new system to house the personal data of its employees. The problems of the old system have been taken into account in the specifications of the replacement system. ██████████ ██████████ has repeatedly attempted to obtain an opinion on the issue of the log data of the system used on its ships from the authorities, but has not received a reply.

88. In the matter at hand, ██████████ has complied with the deadlines set by the authority and replied to questions as openly and concisely as possible with a view towards resolving this complaint as efficiently as possible from the authority's perspective.

Conclusion

89. ██████████ has stressed that it has not obtained any indirect or direct financial advantage from the events under investigation. According to the company's response, ██████████ is more likely to incur financial losses from the incident due to reputation damage.

90. The total turnover of ██████████ was EUR 258,243,347.47 in 2021. In this context, the company stressed that the tourism industry suffered badly from the consequences of the coronavirus pandemic. The authority was requested to take the above into consideration when deciding on sanctions.

91. Finally, ██████████'s response maintained that an administrative fine should not be imposed for conduct that may have been in violation of the provisions of the Act on the Protection of Privacy in Working Life or other legislation apart from the General Data Protection Regulation, nor should considerations based on such other legislation be taken into account as grounds for increasing the administrative fine.



Assessment of cross-border processing

92. The GDPR contains specific provisions on the processing of matters with a cross-border dimension as defined in Article 4(23). Such matters must be processed by a competent supervisory authority as provided for in Article 56 and Chapter VII of the GDPR.
93. In its response, [REDACTED] has announced that it is the controller with regard to the processing discussed herein. [REDACTED]'s head office is in Finland, and the Group also includes [REDACTED] and [REDACTED] based in Sweden, [REDACTED] based in Estonia, [REDACTED] based in Germany, as well as [REDACTED] based in Finland. The operations of all of the aforementioned companies involve the processing of personal data. Their information systems can be accessed from ships. The ships sail on the territorial waters of Finland, Sweden and Estonia as well as on international waters. The group has ships sailing under the Finnish, Swedish and Estonian flags. The complainant has only worked on vessels sailing under the Finnish flag. The German office only employs one person, and the data files discussed herein are not used in Germany, nor is the data of the German employee processed in them.
94. [REDACTED]'s central administration is located in Finland. According to the company, decisions regarding the processing discussed herein are made at the offices of this central administration. Furthermore, [REDACTED] has stated that the central administration also has the power to implement decisions related to the processing discussed herein.
95. The Office of the Data Protection Ombudsman will deal with the matter in accordance with the procedure laid down in Article 60 of the GDPR in cooperation with the supervisory authorities of the participating Member States. In the present case, the concerned supervisory authorities (hereinafter also: "CSAs") within the meaning of Article 4(22)(b) of the GDPR are the supervisory authorities of Sweden, Norway and Estonia, since the processing affects or is likely to significantly affect data subjects in these Member States.
96. The decision includes sections which are subject to the obligations and rules established in the Finnish national legislation following from Article 6(1)(c) of the GDPR. In accordance with Article 55(2) of the GDPR, the Office of the Data Protection Ombudsman is of the view that those sections are not subject to the cooperation mechanism established in Article 60 of the GDPR. Furthermore, the decision includes sections which are subject to the national legislation implementing Article 88 of the GDPR.

Proceedings in the cooperation mechanism

97. In accordance with Article 56 and Article 60(3) of the GDPR, the Office of the Data Protection Ombudsman as the lead supervisory authority, has 21 March 2022 provided relevant information on the matter to the CSAs while its position as lead supervisory authority was established.



-
98. The draft decisions of the Data Protection Ombudsman and the Collegial Body for Sanction has been submitted to the CSAs on 10 November 2022 in accordance with Article 60(3) of the GDPR.
99. The CSAs have not made any comments or objections to the draft decision. Accordingly, the draft decision has been approved.¹ The Office of the Data Protection Ombudsman adopts and notifies the decision to the main establishment of the controller. In addition to this the Office of the Data Protection Ombudsman will inform the complainant, the other supervisory authorities as well as the European Data Protection Board of the decision.²

Applicable law

100. The processing of personal data is provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR). The GDPR has been in force from 25 May 2018. As a regulation, the enactment is directly applicable legislation in the Member States. The rights of the data subject are provided for in Chapter III of the GDPR. The GDPR is specified by the Data Protection Act (1050/2018).
101. More detailed provisions on the processing of health information at the workplace are provided in sections 3 and 5 of the Act on the Protection of Privacy in Working Life (759/2004, Working Life Privacy Act). The storage and recording of patient information is provided for in section 12 of the Act on the Status and Rights of Patients (785/1992; Patient Act) and in the Decree of the Ministry of Social Affairs and Health on Patient Documents (298/2009; Patient Document Decree).
102. The Act on Ships' Medical Stores (584/2015) provides for measures intended to ensure the availability of appropriate first aid and medical care to ships' crews in the event of illness or accident on board.
103. The work of health care professionals is provided for in the Act on Health Care Professionals (559/1994). The Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021, Client Data Act) provides for the secure processing of client data generated by the social welfare and health care services and welfare data generated by the clients themselves for the purpose of the arrangement and provision of health care and social welfare services. The previous version of the aforementioned Act (159/2007, repealed on 1 November 2021) also has significance in this matter.

Legal question

104. As referred to above, the Deputy Data Protection Ombudsman assesses and decides on the applicant's matter based on the General Data Protection Regulation (EU) 2016/679 and the aforementioned special enactments. The matter involves the following legal questions:

¹ Article 60(6) of the GDPR.

² Article 60(7) of the GDPR.



- i. Has [REDACTED] complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnoses into the MAPS system?
- ii. Has [REDACTED] complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when storing data concerning the health of its employees?
- iii. Has [REDACTED] taken every reasonable step in accordance with Article 5(1)(d) and Article 25(1) of the GDPR to ensure that the employee health data processed by it is accurate and up to date?
- iv. Has [REDACTED] provided the data subjects with the information provided for in Article 13 of the GDPR when it has obtained personal data from the data subjects?
- v. Has [REDACTED] complied with the provisions of Article 5(1)(b) of the GDPR when disclosing the complainant's personal data to the police?
- vi. Has [REDACTED] fulfilled the applicant's right of access as provided for in Article 12(3) and Article 15 of the GDPR?
- vii. Should the controller be ordered to comply with the complainant's request to access the data in the user log under Article 58(2)(c) of the GDPR?

Decision of the Deputy Data Protection Ombudsman

Decision

105. The Deputy Data Protection Ombudsman finds that [REDACTED] has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnoses into the MAPS system.
106. The Deputy Data Protection Ombudsman finds that [REDACTED] has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when storing its employees' health information in the MAPS system.
107. The Deputy Data Protection Ombudsman finds that there was a basis for processing patient information.
108. The Deputy Data Protection Ombudsman finds that [REDACTED] has not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR in order to ensure that the personal data processed in the MAPS system is accurate and up to date.
109. The Deputy Data Protection Ombudsman finds that [REDACTED] has not complied with the provisions of Article 5(1)(a) and Article 13 of the GDPR.



-
110. The Deputy Data Protection Ombudsman does not consider themself competent to assess the existence of possible grounds for disclosure of data to the police more extensively than described in the grounds for this decision.
111. The Deputy Data Protection Ombudsman finds that [REDACTED] has not complied with the provisions of Article 12(3) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR.
112. The Deputy Data Protection Ombudsman finds that [REDACTED] has not complied with the provisions of Article 15(1) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR.
113. The Deputy Data Protection Ombudsman does not issue an order to comply with the complainant's request for access to the user log data.

Order

114. The Deputy Data Protection Ombudsman orders the controller to bring its practices for informing the data subjects into compliance with the provisions of the GDPR under Article 58(2)(d) of the GDPR.

Notes

115. The Deputy Data Protection Ombudsman reprimands [REDACTED] under Article 58(2)(b) of the GDPR. The Deputy Data Protection Ombudsman points out that the measures taken by the controller to fulfil the rights of the complainant are not complied with the provisions of Article 12(3) of the GDPR, nor has the controller fulfilled the complainant's request to access her data pursuant to Article 15 of the GDPR. With regard to the accuracy of the data, the controller has not complied with the provisions of Article 5(1)(d) and Article 25(1) of the GDPR. Furthermore, the controller has neglected its duty to inform the data subjects of its processing.

116. The Deputy Data Protection Ombudsman also points out that the controller has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when processing its employees' health information. The Deputy Data Protection Ombudsman notes that the controller's conduct has been particularly reprehensible in this respect. Not only has the processing violated the provision of the aforementioned enactment, but it has also been quite extensive, and the processing cannot be said to have been short in duration. Furthermore, taking into account the subordinate position of the employees with regard to the employer, the processing can be considered to have caused an especially high risk.

Grounds

Processing of employees' health information at the workplace

Facts of the matter



117. According to the response issued in this matter, [REDACTED] has maintained a HR system (MAPS), which has been used to manage employment contracts and perform the employer's obligations. Information related to the employment contract, such as the names and contact details of employees, employment contract status information, qualifications, completed training, as well as information concerning salary payment and health care costs, have been stored in the MAPS system. The MAPS system has also contained information on employee absences, including absences due to illness, complete with dates and ICD diagnosis codes. In addition to the codes, the diagnoses have been recorded in the system in plain text. However, according to the supplement to [REDACTED]'s response, the ICD codes and plain-text diagnoses have been erased from the system in 2020. Such information is no longer contained in the system. At present, only the information that an employee has been absent due to an illness and whether the absence was paid or unpaid or, for example, family leave, is recorded in the system.

Legal evaluation

118. Section 5 of the Working Life Privacy Act provides for the employer's right to process data concerning the health of employees. The employer has the right to process data concerning the employee's health status if the data has been collected from the employee themselves, or elsewhere with the employee's written consent, and the data needs to be processed in order to pay sick pay or other comparable health-related benefits or to establish whether there is a justified reason for absence or if the employee expressly wishes their working capacity to be assessed on the basis of data concerning their health. In addition, the employer has the right to process such data in the specific circumstances and to the stipulated extent separately provided elsewhere in the law. The legislative materials of the enactment preceding the Working Life Privacy Act (Act on the Protection of Privacy in Working Life (477/2001))³ specifically state that the employer has the right to process health information, e.g. medical certificates or statements and the diagnoses given in them, with the employee's consent for the purpose of assessing absences due to illness.⁴

119. Regardless of the employee's consent, the employer is bound by the necessity requirement provided for in section 3 of the Working Life Privacy Act. The employer is only allowed to process personal data directly necessary for the employee's employment relationship, which is connected with managing the rights and obligations of the parties to the employment relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned. No exceptions can be made to the necessity requirement, even with the employee's consent.

120. It should be noted that sick pay practices are frequently based on the provisions of collective agreements. As a rule, such agreements require the employee to deliver a medical certificate with diagnosis information to their employer. In practice, in the case of a recurring illness, the salary payment

³ HE 75/2000 vp, p. 17

⁴ HE 75/2000 vp, p. 24



obligation is often affected by whether the illness is new or a relapse of an existing condition. The provisions on sick pay have accordingly been interpreted to mean that the medical certificate delivered to the employer must include the medical definition of the disease, i.e. the diagnosis. In practice, this means that the employer determines whether the employee's illness entitles them to sick pay.

121. According to section 5, subsection 4 of the Working Life Privacy Act, the employer must store any data in its possession concerning the employee's health separately from any other personal data it has collected. This means that health entries must not be saved into the employer's other personal data files, such as payroll administration registers.

122. The Deputy Data Protection Ombudsman finds that the employer nevertheless has the right to process, for example in its HR systems, data concerning the dates and lengths of an employee's absence from work due to sick leave (acceptable reason, payment of sick pay). However, information on the causes of the absence due to illness, such as the disease or injury or its nature or diagnosis, may not be saved into HR systems. The medical certificates or statements delivered to the employer by the employee must be stored separately from other personal data concerning the employee. Such data may only be processed to the extent and for the purposes provided for in section 5 of the Working Life Privacy Act. Such purposes are usually specific and as well as different for each absence due to illness. In other words, the provisions of the Working Life Privacy Act do not permit or entitle the employer to keep separate health data files on its employees for the purpose of collecting and storing employee health data, such as diagnoses.

123. Based on the above, the Deputy Data Protection Ombudsman finds that the controller has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnosis information into the MAPS system. Since the diagnoses have since been erased from the MAPS system, the Deputy Data Protection Ombudsman does not issue an order to [REDACTED] in this regard.

Storage of employee health information

Facts of the matter

124. The complainant has maintained that [REDACTED] has stored her health information (including diagnoses) in the MAPS system for 20 years.

125. According to [REDACTED]'s response, it has maintained two data files for internal use (the MAPS HR management system and the Medakt patient record system), which have contained employees' health information, among other things.

126. [REDACTED] has said that MAPS is its HR management system used to manage employment contracts and fulfil the employer's obligations, such as salary payment. The Medakt system, on the other hand, has been described by [REDACTED] as an electronic patient record system used on its vessels, into



which the ship's nurses licensed by the National Supervisory Authority for Welfare and Health (Valvira) record the procedures performed on patients and the medicines dispensed to them, as required by section 12, subsection 1 of the Act on the Status and Rights of Patients (785/1992). Patients can include both passengers and crew members who have fallen ill during the voyage.

127. [REDACTED]'s response maintains that sick leave certificates are stored for as long as required for fulfilling the rights and performing the obligations related to the employment relationship. The response also stated that information on absences due to illness and the right to pay is stored in the MAPS system for ten years from the end of the absence. According to the controller, all ICD codes and diagnoses were erased from the MAPS system in 2020.

128. At the moment, the data in the Medakt system is being stored for an indefinite period. According to the information provided, the health information is saved because it has been considered necessary for monitoring the employees' health. Information on an employee's injuries or health problems can be needed later, for example for the processing of insurance cases or occupational disease surveys. The Medakt system contains information from 2012.

Legal evaluation

129. As provided for in section 5, subsection 4 of the Working Life Privacy Act, data concerning health shall be erased immediately after the grounds for processing referred to in section 5, subsection 1 of the said Act have ceased to exist. As stated in the grounds under the previous legal question, the purposes of medical certificates or statements or other documents containing health information, delivered by an employee to the employer, are usually separate as well as specific to each individual absence due to illness. As a rule, the appropriate storage period for such data is thus comparatively short. As further provided in section 5, subsection 4 of the Working Life Privacy Act, the grounds and necessity of processing employee health information shall be evaluated at least every five years.

130. Section 9 of the Act on Ships' Medical Stores provides for the medical journal to be kept of ships' medical stores. According to the provision, all acquisitions made to the medical store, any drugs dispensed to patients and all performed procedures, as well as drugs and medical supplies removed from the medical store shall be entered in the medical journal. All personal data must be stored separately from the information regarding drugs and medical supplies. The medical journal must be preserved for at least five years after the last entry.

131. The Deputy Data Protection Ombudsman interprets the Act on Ships' Medical Stores to be a health and safety statute intended to improve medical care on board ships, rather than a statute on the processing of patient information as such. Section 1 of the Act on Ships' Medical Stores provides for the purpose of the Act. The purpose of the Act on Ships' Medical Stores is to ensure that members of a ship's crew have the possibility to receive appropriate first aid and medical care on board the vessel in case of illness or injury. Accordingly, the Act obliges the shipowner to ensure that the ship carries the drugs and medical supplies provided



for in the Act. Section 9 of the Act on Ships' Medical Stores also makes it possible to process personal data in medical journals. In addition, when treatment procedures are due to a transfer of duties performed by a health care professional as referred to in section 5, subsection 3 of the Act on Ships' Medical Stores, the obligation of a health care professional referred to in section 12 of the Act on the Status and Rights of Patients to prepare and retain patient documents as well as other provisions on the processing of patient records shall be taken into account.

132. Based on the above, the Deputy Data Protection Ombudsman finds that [REDACTED] has not presented any grounds by virtue of which the complainant's data could have been stored for 20 years in the MAPS system. Neither has [REDACTED] presented any justification for retaining the health information of its employees in the MAPS system for ten years from the end of the absence. The controller has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when storing health information on its employees in the MAPS system. Since the diagnoses have since been erased from the MAPS system, the Deputy Data Protection Ombudsman does not issue an order to [REDACTED] in this regard.

133. According to section 2, subsection 1, paragraph 1 of the Patient Act, the term 'patient' is used of a person who uses health care services or is otherwise an object of them. The legislative materials for the Act refer to an established interpretation of the Patient Injury Act, according to which 'health care and medical care' refers to procedures intended to determine an individual's state of health or to restore or maintain their health, performed by health care professionals or in a health care unit. 'Health care professional' refers to an individual operating based on a legal right or legally licensed by the Social Welfare and Health Administration (currently the National Supervisory Authority for Welfare and Health Valvira).⁵ More detailed provisions on health care professionals are laid down in the Act on Health Care Professionals. The legislative materials for the aforementioned Act also state that, in unclear cases, the nature and purpose of the operations and the training of the individual providing treatment can be used to determine whether the activity constitutes health care or medical care for the individual.⁶ In other words, treatment does not have to be provided in an actual health care unit to meet the definition of health care or medical care, provided that the treatment is provided by a health care professional.⁷ For example, health care or medical care provided by a health care professional in a social welfare unit and the services provided by pharmaceutical professionals in pharmacies fall under the scope of the Act.⁸

134. [REDACTED]'s response states that the nurses working on its ships are health care professionals licensed by the National Supervisory Authority for Welfare and Health (Valvira). Based on the above, the Deputy Data Protection Ombudsman finds that individuals making an appointment with a ship's nurse are

⁵ HE 185/91 vp, p. 13.

⁶ HE 185/91 vp, p. 13.

⁷ HE 185/91 vp, p. 14.

⁸ HE 185/91 vp, p. 14.



patients as referred to in the Patient Act, while the entries made by the nurses concerning such individuals are patient documents as referred to in the Patient Act.

135. With regard to the actual patient record entries made in the Medakt system, it is noted that the storage of patient information is provided for in the Patient Act and Patient Record Decree. According to section 2, subsection 1, paragraph 5 of the Patient Act, the term 'patient documents' means the documents or technical records used, drawn up or received when the treatment of the patient is arranged and carried out and which contain information on their state of health or otherwise personal information about the patient. According to section 12 of the Patient Act, health care professionals shall record in patient documents the information necessary for the arranging, planning, providing and monitoring of care and treatment for a patient. According to the provision, patient documents shall be stored for a period necessary for arranging and providing care and treatment for a patient, for investigating possible claims for compensation, and for scientific research. Patient documents shall be disposed of immediately after there are no grounds as referred to above for keeping them. Further provisions on keeping patient documents and their storage periods are laid down in the Patient Documents Decree. The storage periods are defined in the Annex to the Decree. As a rule, patient documents shall be kept for 12 years from the patient's death or, if no information on it is available, for 120 years from the patient's birth.

136. Keeping a medical journal and processing the personal data contained in it is based on section 9 of the Act on Ships' Medical Stores, which defines the information to be stored in the medical journal. Thus, there is a justification for the processing of personal data to be included in the medical journal. According to section 5 of the Act on Ships' Medical Stores, a ship must have the capability to provide first aid and medical care to those in need, among other things, and according to subsection 3 of the said section, responsibility for the administration of first aid and medical care, among other duties, can be assigned to a health care professional. In such cases, the health care professional is obliged to draw up patient document entries for the care or treatment provided as stipulated in section 12 of the Act on the Status and Rights of Patients. The controller has thus had a valid basis for processing patient information.

Data inaccuracy

Facts of the matter

137. The complainant has maintained that some of her information saved in the MAPS system has been partially inaccurate. The complainant has maintained that, for example the ICD code entered into the MAPS system for her sick leave granted at the turn of 2016–2017 does not correspond to the code on the sick leave certificate.

138. According to the controller's response, investigation of the matter revealed that not all ICD codes could be saved into the MAPS system in 2001. In other words, only a portion of the codes was used. It has thus been possible that absences due to illness may have been saved into the system with different codes than those in the actual diagnosis based on which the sick leave was granted. It is



said that the system's users have sought to determine the closest corresponding code that could be entered into the system.

Legal evaluation

139. Article 5 of the General Data Protection Regulation provides for the principles of processing personal data. According to Article 5(1)(d), personal data shall be accurate and, where necessary, kept up to date. The controller must 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 ('accuracy').
140. The data subject has the right to be assessed based on accurate data. Inaccurate personal data can cause a risk to the rights and freedoms of the data subject. Article 16 of the GDPR accordingly provides for the data subject's right to rectification. Data subjects have the right to demand from the controller the rectification of inaccurate personal data concerning them without undue delay. The purpose of this is to prevent the making of incorrect conclusions or decisions based on inaccurate or incomplete data. Inaccurate data means false data that does not correspond to the facts.
141. The provisions of Article 25(1) of the GDPR also have significance in this regard. 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 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 of 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.
142. The European Data Protection Board has issued practical guidelines⁹ on the data protection by design and by default referred to in Article 25 of the GDPR. Among other things, these guidelines describe key considerations regarding accuracy in data protection by design and by default. Such considerations mentioned in the guideline include the degree of accuracy, continued accuracy and data design. The controller shall use technical and organisational design features to decrease possible inaccuracy related to personal data, for example by presenting concise predetermined choices instead of free text fields.¹⁰
143. According to the controller's response, diagnose information was entered into the MAPS system with ICD codes. However, the MAPS system did not have

⁹ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020.

¹⁰ Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, Adopted on 20 October 2020, pp. 24–25.



all of the possible ICD codes available for selection, which has enabled incorrect diagnosis entries.

144. Based on the above, the Deputy Data Protection Ombudsman finds that the controller has not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR to ensure the accuracy of the personal data processed in the MAPS system. Since diagnosis information is no longer being entered into the MAPS system, the Deputy Data Protection Ombudsman will not issue any orders to [REDACTED] concerning the infringement here established.

Informing the data subjects

Facts of the matter

145. According to the complainant, employees have not been informed in any way of the extensive data files discussed herein. No information or instructions related to the controller's processing of its employees' personal data has been available on the company intranet.

146. [REDACTED]'s response noted that investigation into the matter showed that employees have not been sufficiently informed of the processing discussed herein.

Legal evaluation

147. According to Article 5(1)(a) of the General Data Protection Regulation, personal data shall be processed in a transparent manner in relation to the data subject. Article 12 of the GDPR lays down more detailed provisions on transparency. The principle of transparency is strongly linked to Article 13 of the GDPR, which provides for the information to be provided to the data subject where personal data is collected from the data subject themselves.

148. It should be noted that the Article 29 Working Party has issued practical guidelines¹¹ ('Transparency Guidelines') on the principle of transparency. These guidelines note that the transparency obligation applies to three central areas: 1) the provision of information to data subjects related to fair processing; 2) how data controllers communicate with data subjects in relation to their rights under the GDPR; and 3) how data controllers facilitate the exercise by data subjects of their rights.

149. It should also be noted that the GDPR does not provide for the form in which the data should be provided or other details. However, the Regulation provides that the controller is obliged to implement "appropriate measures" to provide the information required by transparency to the data subject.¹² This means that the controller must take into account all circumstances of the collection and processing of the personal data when choosing an appropriate method and form

¹¹ Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018).

¹² See GDPR, Article 12(1).



for informing the data subjects. In particular, appropriate measures will need to be assessed in light of the product/ service user experience.¹³

150. The data subject should be informed of the scope and consequences of the processing in advance, so that the ways in which the personal data are used will not come as a surprise to the data subject later. This is also important in view of the principle of fairness referred to in Article 5(1) of the GDPR and is related to recital (39), according to which natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data.

151. In the case of personal data collected from the data subject themselves as referred to in Article 13 of the GDPR, the information listed in the Article must be provided to the data subject at the time when the data is obtained from the data subject.

152. Regarding the form in which the data is to be provided, it can be stated that, according to Article 13 of the GDPR, the controller shall "provide the data subject with all of the following information [...]" . The wording "provide" is relevant here. This means that the data controller must take active steps to furnish the information in question to the data subject or to actively direct the data subject to the location of it.¹⁴

153. According to the complainant, the data subjects have not been informed in any way of the data files described herein. The controller has not denied this claim. The controller has admitted that the data subjects have not been informed adequately. The Deputy Data Protection Ombudsman thus finds that the controller has not complied with the provisions Article 5(1)(a) and Article 13 of the GDPR.

154. The Deputy Data Protection Ombudsman orders the controller to bring its practices for informing the data subjects into compliance with the provisions of the GDPR under Article 58(2)(d) of the GDPR.

Disclosure of personal data to the police

Facts of the matter

155. The data recorded in the MAPS system has been used for HR management, such as salary payment and the verification of its accuracy. The diagnosis information entered into the system was originally processed to determine the employee's eligibility for pay during their absence. However, [REDACTED] [REDACTED] has since assessed that entering diagnoses into the system is not necessary in view of the purpose of the system. As described above, the Medakt system is an electronic patient record system used on [REDACTED]'s

¹³ Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018), p. 14.

¹⁴ Guidelines on transparency under Regulation 2016/679, WP260 rev.01 (Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018), p. 18.



vessels. According to the information provided, data from the files has not been used for purposes other than the original purpose of processing.

156. Regardless of the above, [REDACTED] has stated that the complainant's health information has been disclosed to the police for the investigation of a criminal matter. According to [REDACTED]'s response, this was not a correct course of action. The controller continued by stating that, in a pre-trial investigation, a physician or other health professional can be obliged to testify on secret patient information, for example in case of an offence for which the maximum sentence is at least six years of imprisonment. However, the criminal matter referred to herein did not involve such an offence. The controller continues by stating that the information should not have been disclosed for the criminal investigation without the patient's specific written consent.

Legal evaluation

157. According to Article 5(1)(b) of the General Data Protection Regulation, personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation'). Recital (50) of the GDPR likewise states that the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected.

158. As stated in the grounds under the first legal question, the employer is, as such, entitled to also process diagnosis information related to its employees' absences due to illness. However, the purposes for such processing are separate as well as specific to each period of absence. The purpose of processing patient information, on the other hand, is related to the patient's treatment, while the purpose of processing the data in the medical journal is related to the duties provided for in the Act on Ships' Medical Stores.

159. According to section 14 of the Patient Act, punishment for breaching the secrecy obligation referred to in paragraph 2 and in point 5 of paragraph 3 of section 13, shall be imposed according to section 1 or 2 of chapter 38 of the Criminal Code, unless the offence is punishable under section 5 of chapter 40 of the Criminal Code, or unless a more severe punishment is prescribed for it elsewhere in the law. Since information on the complainant's diagnoses was later disclosed to the police, the Deputy Data Protection Ombudsman finds that the basis for the disclosure may be assessed as a criminal matter. The Deputy Data Protection Ombudsman thus does not consider themselves competent to assess the existence of a possible basis for disclosure to any greater extent. The complainant may turn to the police in this matter.

Right of access

Facts of the matter

160. According to the complainant, she has requested access to her personal data from [REDACTED] at least on 10 January 2020 and 3 February 2020.



161. According to the information provided by [REDACTED], the information on the complainant's sick leave certificates was given to the complainant insofar as it was available. According to [REDACTED], it had already erased the oldest data. Copies of the remaining sick leave certificates were delivered to the complainant on 1 April 2020. Before this, the complainant's questions had been answered by email at least on 31 January 2020. Diagnosis information was not provided to the complainant in this connection.

162. However, in this respect, the complainant has referred to a copy of her diagnosis information entered into the MAPS system that she acquired in 2020 and delivered to the Office of the Data Protection Ombudsman. Since the diagnosis information had not actually been erased in 2018–2019, the complainant has stressed that this information could have been provided to her in response to her request made on 10 January 2020.

Legal evaluation

163. Article 15 of the General Data Protection Regulation provides for the data subject's right of access to data. 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 specifically listed in the Article.

164. Furthermore, Article 12 of the GDPR provides for detailed rules regarding the exercise of the rights of the data subject. According to paragraph 3 of the Article, 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. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject. Furthermore, according to paragraph 4 of the Article, 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.

165. In the matter at hand, the complainant had not received the requested diagnosis information in response to her request made on 10 January 2020, even though [REDACTED] was still verifiably in possession of that information on 6 February 2020, when the complainant obtained it by other means.

166. The complainant filed her aforementioned requests in this matter on 10 January 2020 and 3 February 2020. Copies of the remaining sick leave certificates were delivered to the complainant in response to her requests on 1 April 2020. The complainant and the controller's representatives had engaged in email correspondence in the interim. In other words, the controller replied to the complainant's messages and requests within one month of the complainant's



aforementioned requests. However, the controller did not provide the complainant with the information she had requested within that time period. Neither had the controller given the complainant any reason for this delay in providing the information to her. As the controller did not provide the complainant with all of the information requested by her within one month of the complainant's aforementioned first request, the controller did not comply with the provisions of Article 12(3) of the GDPR when replying to a request made pursuant to Article 15 of the GDPR.

167. The complainant had specifically requested the diagnosis information saved into [REDACTED]'s systems from the company on several occasions. The controller can thus be considered to have been aware of the complainant's wish to access precisely that information. Regardless of the above, the information was not delivered to the complainant in an appropriate manner. Even though the complainant eventually gained access to the information through a nurse, [REDACTED] [REDACTED]'s conduct in the matter cannot be considered appropriate. The diagnosis information was not delivered to the complainant in the same connection and through the same channel as the other information provided to her. On the contrary, the complainant was led to believe that there was no diagnosis information separately entered into the system. As the controller did not grant the complainant access to the diagnosis information entered into the system, the controller did not comply with the provisions of Article 15(1) of the GDPR when responding to the complainant's request made pursuant to Article 15 of the GDPR.

Right of access to log data

Facts of the matter at hand and information provided in the response

168. The complainant has requested access to the log data concerning the complainant's personal data from [REDACTED]. The complainant has not been given access to the log data.

169. The response to the request for information referred to the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007) repealed on 1 November 2021. According to section 18 of the said Act, a client has, for the purposes of determining or exercising the client's rights related to the processing of their client information, the right to be informed by the social welfare or health care service provider of who has used or received information concerning the client, as well as the basis for such use or disclosure. Such information shall be based on log register data and provided free of charge and without delay upon written request.

170. The controller has proposed that the obligation to disclose log data would apply to health care service providers, meaning health care units referred to in section 2, subsection 1, paragraph 4 of the Act on the Status and Rights of Patients, employers referred to in section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), as well as self-employed health care professionals. The medical care of ship crews, including on the vessels of [REDACTED], is based on the Act on Ships' Medical Stores. The obligation to enter procedures performed into the medical journal is based on the same Act. Since the Act on the Status and Rights of Patients does not refer to the Act on Ships' Medical Stores,



[REDACTED] has interpreted the provision on the disclosure of log data to mean that it is not a health care service provider as referred to in the Act and has thus considered that it does not have the right to disclose log data. In addition, [REDACTED] has stated that the log data concern the users of information systems and cannot thus be disclosed to the subject of processing by virtue of the GDPR alone.

Legal evaluation (General Data Protection Regulation)

171. Article 15 of the General Data Protection Regulation provides for the data subject's right of access to data. Data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data as well as the information listed in the Article. In other words, a data subject has this 'right of access' to data concerning themselves.

172. According to the Data Protection Ombudsman's established decision-making practice, user log data does not concern customers, but the employees who have processed customer data. Therefore, the data subject's right of access to data has not been considered to apply to user log data. In the absence of special legislation, the right to access user log data has thus been restricted to the individuals who have processed personal data stored in the data file (see, for example, decision EOA 1433/4/05 of the Parliamentary Ombudsman, issued on 8 February 2007 and the Deputy Data Protection Ombudsman's decision in matter 7681/152/2018, issued on 4 August 2020). Notwithstanding the above, customers have had, by virtue of their right of access, the right to access their actual customer data and any entries included in such data.

173. As stated in the decision practice referred to above, log data has been considered to concern the employees who have processed the customer or register data. Therefore, log data has not been considered to constitute data concerning the data subject and has thus been excluded from the right of access provided for in the aforementioned Article 15. It must nevertheless be noted that the aforementioned Deputy Data Protection Ombudsman's decision 7681/152/2018 has been appealed in the Administrative Court of Eastern Finland, which has in turn requested a precedent on the matter from the Court of Justice of the European Union.

Legal evaluation (special legislation)

174. In addition to the right based on Article 15 of the GDPR, it is possible to obtain log data on the basis of the right of access laid down in other legislation. At the time of a request for log data, section 18 of the now-repealed Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (250/2014, repealed by Act 784/2021) laid down provisions on the patient's right to obtain information from the provider of healthcare and social welfare services on who used or to whom the data concerning them has been disclosed and on the grounds for the use or disclosure. This was a special right of access to information separate from the right laid down in the GDPR. The Data Protection Ombudsman was not responsible for assessing this right of access to information under the repealed Act.



Although section 26, subsection 4 of the new Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (784/2021) stipulates this task, the provision only applies to requests made after its entry into force (November 1, 2021). Therefore, the Deputy Data Protection Ombudsman does not assess the fulfilment of this right of access to information in this case.

175. However, the Deputy Data Protection Ombudsman provides general guidance on the matter at the end of this decision.

Applicable legal provisions

As set out in the grounds.

Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court pursuant to the provisions of the Administrative Judicial Procedure Act (808/2019). The appellate court is the Administrative Court of Helsinki.

Instructions for appeal are appended.

Service of notice

Notice of this decision will be served by post against an acknowledgment of receipt pursuant to section 60 of the Administrative Procedure Act (434/2003).

Additional information on this decision is available from the referendary

[REDACTED], tel. [REDACTED].

Guidance by the Deputy Data Protection Ombudsman

The complainant has requested access to the log data concerning the complainant's personal data from [REDACTED]. At least the legislation listed below is relevant to this assessment.

The response issued by [REDACTED] maintained that the obligation to provide log data applies to health care service providers, meaning health care units referred to in section 2, subsection 1, paragraph 4 of the Act on the Status and Rights of Patients, employers referred to in section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), as well as self-employed health care professionals. In the opinion of [REDACTED], on ships such as the vessels operated by [REDACTED], the medical care of the ship's crew is based on the Act on Ships' Medical Stores. The obligation to record procedures performed on patients is also based on the aforementioned Act. Since the Act on the Status and Rights of Patients does not refer to the Act on Ships' Medical Stores, [REDACTED] has interpreted the provision on the disclosure of log data to mean that it is not a health care service provider as referred to in the Act and has thus considered that it does not have the right to disclose log data.

Office of the Data Protection Ombudsman

PL 800, FI-00521 Helsinki, Finland – tel. +358 29 566 6700 (exchange) – tietosuoja@om.fi – www.tietosuoja.fi



In the general opinion of the Deputy Data Protection Ombudsman, shipboard health care cannot, based on the above, be excluded from the scope of all basic statutes applying to the processing of patient information. Since health care professionals perform procedures on individuals on the ship, the Deputy Data Protection Ombudsman is of the opinion that section 12 of the Patient Act regarding the obligation to prepare patient documents in principle applies.

The scope of the Client Data Act is relevant to this question. According to section 2 of the Client Data Act, the Client Data Act lays down provisions that supplement and specify the General Data Protection Regulation when social welfare and health care client data as well as welfare data generated by the client themselves is processed electronically for the purpose of providing health care and social welfare services. As stated in the legislative materials for the Act, the Act applies to the social welfare and health care services organised or provided by public and private social welfare and health care service enablers.¹⁵

According to section 3, subsection 1, paragraph 7 of the Client Data Act, 'service enabler' means an organiser or provider of social welfare and health care services. According to section 3, subsection 1, paragraph 8, point b of the Act, 'service organiser' means a service enabler that, as a private service enabler, has an obligation to ensure that the client receives the service they are entitled to under the agreement. According to section 3, subsection 1, paragraph 9 of the Act, 'service provider' in turn means a service enabler, which a) provides the social welfare or health care service itself in the role of service organiser; and which b) provides a social welfare or health care service on behalf of a service enabler.

'Health care unit' (i.e. service provider) has also been defined in section 2, subsection 1, paragraph 4 of the Patient Act.¹⁶ According to section 7, subsection 1, paragraph 2 of the Occupational Health Care Act (1383/2001), 'service enabler' means both employers and self-employed health care professionals.

According to section 2, subsection 1 of the Act on Private Health Care (152/1990), 'health care services' mean 1) laboratory operations; 2) radiological operations and other comparable examination and imaging methods; 3) other examinations or procedures performed to diagnose an illness or determine treatment; 4) physiotherapeutic operations and other performance-improving and -maintaining procedures and therapies; 5) occupational health care; 6) medical and dental services and other health care, medical care and comparable services; 7) massage; and 8) ambulance services.

According to section 2, subsection 2 of the Act on Private Health Care, 'service provider' means an individual person or company, cooperative, association or other corporation or foundation which maintains a unit that provides health care services. Other self-employed persons or employers who organise the occupational health care services referred to in the Occupational Health Care Act themselves are not considered service providers.

¹⁵ HE 212/2020 vp, p. 74

¹⁶ HE 212/2020 vp, p. 76.



'Self-employed person', on the other hand, is defined in section 2, subsection 3 of the Private Health Care Act as a health care professional referred to in section 2, subsection 1 of the Health Care Professionals Act (559/1994) who practises their profession independently.

According to section 4 of the Act on Private Health Care, a service provider must have a licence granted by the licensing authority for providing health care services. According to section 9a of the Act, a self-employed person must file a written notification of their operations to the State Regional Administrative Agency before providing health care and medical care services referred to in the Act.

For the sake of completeness, we also refer to the written question¹⁷ concerning problems in the interpretation of the Act on Ships' Medical Stores with regard to questions regarding the availability of log data and the patient's right to have their health information recorded, inspected and amended, as well as to the reply to this question given by the Minister of Social Affairs and Health on 17 March 2022¹⁸. The reply states that the Client Data Act is not applied on board ships, because the ship is not a service provider as referred to in the Act. The reply also states that the Ministry of Social Affairs and Health is in the process of preparing an overhaul of social welfare and health care data management regulations, which will, among other things, combine the regulations concerning the processing of client data laid out in the Act on the Electronic Processing of Client Data in Healthcare and Social Welfare and the Act on the Status and Rights of Patients. The reference to secrecy regulations in section 9 of the Act on Ships' Medical Stores will also be updated in this connection. A draft that has already been circulated for comments only proposes to add a reference to the new Act with regard to the secrecy obligation, but the extension of the general obligations concerning the processing of client data, such as secrecy, log data collection and the client's right of access to log data, can still be discussed in the finalisation phase of the draft.¹⁹

Notwithstanding the above, the Deputy Data Protection Ombudsman does not consider themselves competent to decide the question of whether [REDACTED] must be considered a service provider as referred to in section 26 of the Client Data Act. Since, for reasons explained in the decision proper, the Deputy Data Protection Ombudsman is not competent to decide the question of the complainant's right of access to log data in the matter at hand, the Deputy Data Protection Ombudsman has not requested a statement on the matter from the authorities responsible for the enforcement of the Client Data Act. However, the Deputy Data Protection Ombudsman will forward this decision to the National Supervisory Authority for Welfare and Health, State Regional Administrative Agency for Southern Finland and the Ministry of Social Affairs and Health for information and possible further action.

This guidance issued by the Deputy Data Protection Ombudsman is not subject to appeal.

¹⁷ Written question KK 78/2022 vp.

¹⁸ Reply to written question KKV 78/2022 vp

¹⁹ Reply to written question KKV 78/2022 vp, p. 2.



Deputy Data Protection Ombudsman _____

Referendary senior officer _____

The document is signed electronically. The legitimacy of the signature can be verified at the registry of the Office of the Data Protection Ombudsman if necessary.

Appendices

Appeal instructions

Distribution

Complainant

[REDACTED]

Contact information of the Office of the Data Protection Ombudsman

Postal address: P. O. Box 800, FI-00531 Helsinki, Finland

Email: tietosuoja@om.fi

Telephone exchange: +358 (0)29 566 6700

Website: www.tietosuoja.fi

Office of the Data Protection Ombudsman

PL 800, FI-00521 Helsinki, Finland – tel. +358 29 566 6700 (exchange) – tietosuoja@om.fi – www.tietosuoja.fi



Sanctions Board Final Decision on an Administrative Fine

Controller [REDACTED]

1. As indicated in the decision of the Deputy Data Protection Ombudsman, [REDACTED] [REDACTED] has not complied with the provisions of section 5, subsection 4 of the Working Life Privacy Act when saving diagnosis information into the MAPS system or storing its employees' health information in the MAPS system. Neither has [REDACTED] taken every reasonable step in accordance with Article 5(1)(d) and Article 25(1) of the GDPR to ensure the accuracy of the personal data processed in the MAPS system.
2. [REDACTED] [REDACTED] has not complied with the provisions of Article 5(1)(a) and Article 13 of the GDPR. Neither has [REDACTED] complied with the provisions of Article 12(3) nor Article 15(1) of the GDPR when responding to the complainant's request made pursuant to Article 15 of the GDPR.
3. Taking into account the gravity of the infringement in particular, the matter does not consist of a minor infringement as referred to in recital (148) of the GDPR. With regard to effectiveness, proportionality and dissuasiveness and in view of the provisions of Article 83(2) of the GDPR, it must be noted that, in the matter at hand, an order issued by the Deputy Data Protection Ombudsman under Article 58(2)(d) of the GDPR in combination with a reprimand will not be a sufficient sanction in this matter. An administrative fine must be imposed in the matter. The fact that this is not a case of individual infringements of the Working Life Privacy Act and Article 5(1)(a) and Article 13 of the GDPR, but established practices on the part of [REDACTED], also speaks for the imposition of an administrative fine.
4. [REDACTED] has not complied with the following provisions referred to in Article 83(5) of the GDPR, and an administrative fine is imposed for their infringement: 1) Article 5(1), points (d) and (a); 2) Article 13; 3) Article 12(3); and 4) Article 15(1). Neither has [REDACTED] complied with Article 25(1) of the GDPR, which calls for the imposition of an administrative fine pursuant to Article 83(4) of the GDPR.
5. [REDACTED]'s turnover was EUR 258,243,347.47 in 2021. In the matter at hand, the maximum amount of the administrative fine imposed on [REDACTED] [REDACTED] is EUR 20,000,000. The Sanctions Board consisting of the Data Protection Ombudsman and Deputy Data Protection Ombudsmen ('Sanctions Board') orders, in addition to the corrective powers exercised and corrective measures ordered above by the Deputy Data Protection Ombudsman, the controller to pay the State an administrative fine of EUR 230,000 (two hundred thirty thousand) by virtue of Article 58(2)(i) and Article 83 of the General Data Protection Regulation. The Sanctions Board of the Office of the Data Protection Ombudsman finds an administrative fine of EUR 230,000 to be effective, proportionate and dissuasive.



Grounds for imposing the administrative fine

6. Article 83 of the General Data Protection Regulation provides for the general conditions for imposing administrative fines. Firstly, the imposition of administrative fines shall in each individual case be effective, proportionate and dissuasive. Secondly, administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, the corrective powers provided for in Article 58. In the primary matter at hand, the Deputy Data Protection Ombudsman has ordered [REDACTED] to bring its practices for informing data subjects into compliance with the provisions of the GDPR and issued a reprimand to the company. The administrative fine is thus imposed in addition to points (b) and (d) of Article 58(2).
7. Due regard shall be given to the considerations listed in 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.
8. As mentioned above, [REDACTED] has not complied with the following provisions referred to in Article 83(5) of the GDPR, for the infringement of which an administrative fine is imposed: 1) Article 5(1), points (d) and (a); 2) Article 13; 3) Article 12(3); and 4) Article 15(1). Neither has [REDACTED] complied with Article 25(1) of the GDPR, which calls for the imposition of an administrative fine pursuant to Article 83(4) of the GDPR.
9. According to Article 83(3) of the GDPR, if a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
10. The gravity of the infringements shall be assessed on the basis of the considerations listed in Article 83(2) of the GDPR. The assessment must identify the conduct or neglect that can be considered the most reprehensible in view of the details of the matter under assessment.
11. In the matter at hand, the infringements of Articles 5, 13, 12 and 15 of the GDPR, as well as the infringement of obligations arising from Member State legislation adopted in accordance with Chapter IX of the GDPR, are the most serious and fall within the higher administrative fine category provided for in Article 83(5) of the GDPR. The applicable maximum amount of the administrative fine is thus determined pursuant to Article 83(5) of the GDPR and may not be exceeded by virtue of Article 83(3) of the GDPR.
12. Infringements of the provisions of points (a) (Articles 5, 6, 7 and 9) and (b) (Articles 12 to 22) of Article 83(5) shall, in accordance with Article 83(2), be subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.



-
13. The Guidelines of the Article 29 Working Party²⁰ on the application and setting of administrative fines were also given due regard in the assessment of the matter.

Assessment of the gravity of the infringements

14. Due regard was given to points (a), (b) and (g) of Article 83(2) in the assessment of the gravity of the infringements.

Nature, gravity and duration; nature, scope or purpose of the processing

15. According to recital (51) of the GDPR, personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Special requirements have accordingly been set for the processing of special categories of personal data, including that such personal data should not, as a rule, be processed. The processing of such personal data is only permitted when both 1) one of the general requirements for processing provided for in Article 6 of the GDPR is met; and 2) one of the special conditions for processing provided for in Article 9 of the GDPR applies.

16. Even though [REDACTED] has not processed its employees' health information without meeting the requirements provided for such processing in Articles 6 and 9 of the GDPR in this matter, [REDACTED] has processed data concerning the health of its employees in violation of the provision of section 5, subsection 4 of the Working Life Privacy Act. In addition, [REDACTED] has failed to comply with the provisions of Article 5(1)(d) and Article 25(1) of the GDPR. It should be noted that data protection by design and by default is one of the core elements of the GDPR on which the implementation of data protection is founded in practice.

17. Several infringements and shortcomings have been identified in the matter. In addition to the aforementioned infringements, [REDACTED] has failed to comply with the provisions of Article 5(1)(a) and Article 13 of the GDPR. This right constitutes a right to information, which enables, for example, the exercise of the rights of the data subject provided for in the Regulation. The Sanctions Board finds an infringement of this right to be especially reprehensible.

18. Neither has [REDACTED] complied with the provisions of Article 12(3) nor Article 15(1) of the GDPR when responding to the complainant's request made pursuant to Article 15 of the GDPR. With regard to the latter, however, due regard was given in the assessment to the fact that [REDACTED] and the complainant had engaged in email correspondence regarding the matter, demonstrating that the company attempted to respond to the complainant's request within the prescribed time limit. Due regard was also given to the fact that the infringement of Article 12(3) and Article 15(1) of the GDPR was limited

²⁰ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017).



to the individual case discussed herein. No information on large-scale infringements of the aforementioned legal provisions has come to light in the matter.

19. It must be specifically noted that the Working Life Privacy Act has been in force since 2004 and application of the GDPR began in 2018. [REDACTED] has thus had a reasonable amount of time to bring the processing activities discussed herein to compliance with the law, and the infringements cannot be said to have been brief in duration.
20. Furthermore, taking into account that the incompleteness of the ICD codes available in the MAPS system only applied to 2001, the period of time during which data may have been inaccurate can nevertheless be considered relatively short with regard to the matter as a whole. However, this does not have a mitigating effect on the assessment of the matter, as there was no legitimate basis for recording ICD codes. Instead, the fact that even incorrect diagnosis data have been retained for a considerable period of time is taken into account in the assessment as an aggravating factor. The processing of erroneous diagnosis data poses a high risk to the legal protection of data subjects.
21. It should be noted that the nature of the infringements must be considered to speak in favour of imposing an administrative fine.

Number of data subjects affected by the infringement and the level of damage

22. The MAPS system is said to contain the personal data of approximately 6,000 data subjects. Some of these data subjects are current employees of [REDACTED] and some are former employees. None of the parties have claimed that the infringements related to the MAPS system would only apply to a limited group of the data subjects. On the contrary, the infringements discovered reflect a systematic approach and lack of appropriate practices. The processing has affected a significant part of [REDACTED]'s personnel.
23. In the assessment of the impact of the infringements on the number of data subjects, due regard was also given to the fact that the processing discussed herein was not limited to a national scale, but has also affected data subjects in the area of the EU/EEA who have worked on [REDACTED]'s vessels sailing under the Finnish flag. The processing has affected data subjects in a vulnerable position in relation to [REDACTED].
24. The infringements were not single or isolated incidents. The number of data subjects affected by the infringements cannot be considered minor. On the one hand, this number reflects the gravity of the infringements but, on the other hand, no financial damage to the data subjects can be established based on the information provided to the Office of the Data Protection Ombudsman.
25. It should be noted that the number of data subjects affected by the infringements must be considered to speak in favour of imposing an administrative fine in the matter. On the other hand, the fact that the data



subjects have not been proven to have suffered concrete financial or other material damage as a consequence of the infringements can be taken into account as a factor reducing the amount of the administrative fine in the matter.

The intentional or negligent character of the infringement

26. According to the aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines, 'intent' generally requires knowledge and wilfulness in relation to the infringement, while 'unintentional' means that there was no intention to cause the infringement although the controller 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.²¹
27. The response to the hearing maintained that the matter at hand did not involve intentional infringements. Also according to the response, the controller had not actively made a knowing decision to, for example, keep inaccurate data in the employee register. The response compares the situation to human error, due to which the system containing the personal data had not been updated to comply with the legislation in force. We again refer to the aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines. The guidelines state that human error or, for example, failure to apply technical updates in a timely manner may be indicative of negligence. It should also be noted that it is well established in Finland that ignorance of the content of the law does not in general mean the kind of mistake that would eliminate possible intentionality or negligence. The controller is responsible for ensuring that its operations comply with the provisions of the law. Notwithstanding the above, with regard to the infringements of section 5, subsection 4 of the Working Life Privacy Act, the Sanctions Board finds no cause to assess the matter differently than [REDACTED] did in its response to the hearing. [REDACTED] has announced that it had taken corrective measures even before the Office of the Data Protection Ombudsman began its investigation into the matter. It was also taken into account in the assessment that [REDACTED] had already taken corrective measures based on communication with a single data subject. When assessing the matter as a whole, the Sanctions Board finds that [REDACTED]'s infringements assessed in this paragraph cannot be considered intentional or negligent.
28. The response to the hearing referred to the email correspondence between [REDACTED] and the complainant, regarding the complainant's right of access to her data. Even though [REDACTED] did not fulfil the right within the prescribed one-month time limit, the aforementioned correspondence demonstrates that [REDACTED] nevertheless sought to fulfil the complainant's right in a timely manner. On the other hand, the Sanctions Board considers it especially reprehensible that, regardless of the complainant's specific request to access her diagnosis information, this information was not delivered to the complainant. Such conduct is indicative of at least negligence.

²¹ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 12.



However, when assessing the aggravating and mitigating factors affecting the amount of the administrative fine, the Sanctions Board does not give weight to the above-mentioned fact. However, for the sake of clarity, it should be noted that the imposition of an administrative fine is not subject to the condition that the infringement found is intentional or negligent. The intentional or negligent nature of the infringement is only one of the factors which, as provided for in Article 83(2) of the GDPR, must be duly taken into account when deciding on the imposition of an administrative fine and the amount of the administrative fine.

29. With regard to the infringement of Article 5(1)(a) and Article 13 of the GDPR established in the primary matter, it should be noted that this was not a case of providing insufficient or incomplete information to data subjects. Rather, the information provided for in the GDPR was not delivered to the data subjects at all. In this regard, [REDACTED]'s conduct indicates that the company has not sufficiently familiarised itself with the legislation in force and the requirements arising therefrom, which consequently indicates contempt for the provisions of the law.

The categories of personal data affected by the infringement

30. As noted above, the infringements established in this matter affected data concerning the health of the data subjects. The Sanctions Board has already assessed the significance of infringements involving such data to the assessment of sanctions under "Nature, gravity and duration; nature, scope or purpose of the processing" above.

Assessment of aggravating and mitigating factors

Measures taken by the controller to mitigate the damage caused to the data subject

31. According to the aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines, the controller should do everything in its power to mitigate the consequences of the infringement to the affected parties. According to the guideline, the supervisory authority may take such responsible behaviour or the lack of it into account in the calculation of the administrative fine.²²
32. [REDACTED] has announced that it took corrective measures after the complainant had contacted the company. According to the company, it had started looking into the matter even before the Office of the Data Protection Ombudsman began its investigation. As mentioned above, it is also significant that, according to [REDACTED], it took corrective measures immediately after being contacted by a single data subject. The Sanctions Board commends such a proactive approach.

²² Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 12.



The degree of responsibility taking into account technical and organisational measures implemented by the controller pursuant to Article 25

33. As provided for in Article 25 of the GDPR, the controller shall take into account in its operations "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".
34. The response to the hearing stressed that [REDACTED] has ensured that the personal data in question can only be accessed by individuals whose duties have been directly related to the data and who have required the data in their work. In other words, access rights have been managed to ensure that the data is only processed by authorised persons. [REDACTED] has stated that it has implemented the principles of integrity and confidentiality by logging events in the information systems, for example.
35. Regardless of the measures taken, it was not possible to save all ICD codes into the MAPS system in 2001. In other words, only a portion of the codes was used. It has thus been possible that absences due to illness may have been saved into the system with different codes than those in the actual diagnosis based on which the sick leave was granted. This error was only discovered later, when the matter was looked into after the complainant had contacted the company. As mentioned above, [REDACTED]'s announcement that it has taken corrective measures after being contacted by the complainant and before the Office of the Data Protection Ombudsman launched its own investigation into the matter must be taken into account to the company's benefit. In other words, [REDACTED] can be considered to have taken timely measures to stop the discovered infringement soon after the company became actively aware of it. The Sanctions Board gives due regard to this as a mitigating factor in its assessment.

Any relevant previous infringements and measures ordered with regard to the same subject-matter

36. The aforementioned Guidelines of the Article 29 Working Party on the application and setting of administrative fines also state that the supervisory authority should assess the track record of the unit guilty of the infringement. The supervisory authority should consider that the scope of the assessment here can be quite wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be "relevant" for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.²³
37. The Data Protection Ombudsman is not aware of any prior infringements of data protection regulations by [REDACTED]. Neither have measures

²³ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 15.



referred to in Article 58(2) of the GDPR been ordered against [REDACTED] [REDACTED] in the past for the infringements discussed herein. The Sanctions Board does not find the above to be either a mitigating or aggravating factor in the assessment of sanctions.

Degree of cooperation with the supervisory authority and the manner in which the infringement became known to the supervisory authority

38. According to the Guidelines of the Article 29 Working Party on the application and setting of administrative fines, the degree of cooperation may be given "due regard" when deciding whether to impose an administrative fine and in deciding on the amount of the fine. It can be relevant to the assessment of cooperation with the supervisory authority whether the controller has responded to the supervisory authority's requests during the investigation in a manner that has significantly limited the risk to the rights of natural persons. That said, the guidelines state that it would not be appropriate to give additional regard to cooperation that is already required by law.²⁴
39. As provided for in Article 31 of the GDPR, the controller shall cooperate, on request, with the supervisory authority in the performance of its tasks. The controller also has an obligation under Article 58(1) of the GDPR and section 18 of the Data Protection Act to deliver the requested information to the supervisory authority.
40. The supervisory authority has learned of [REDACTED]'s infringements through a complaint. In its consideration of a reasonable sanction, the Sanctions Board has given due regard to the fact that [REDACTED] has responded to the authority's requests for information within the time limit. [REDACTED] [REDACTED] has been cooperative with the Office of the Data Protection Ombudsman. However, the Sanctions Board does not consider the aforementioned to be either a mitigating or aggravating factor in the assessment of sanctions.

Any other aggravating or mitigating factor applicable to the circumstances of the case

41. In assessing the amount of the administrative fine, the Sanctions Board gives due regard to the damage suffered by the tourism industry from the effects of the coronavirus pandemic.
42. As mentioned above, the controller has also taken action to remedy the shortcomings identified in this matter largely on its own initiative. The shortcomings in the fulfilling the rights of the data subject can be considered to concern the individual case discussed herein. Nothing that would indicate systematic infringements of the GDPR by the controller in this regard has been brought forward in the matter.

²⁴ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 (WP 253, Adopted on 3 October 2017), p. 15.



Conclusion

43. According to [REDACTED]'s response to the hearing, an administrative fine should not be imposed for conduct that may have violated the provisions of the Working Life Privacy Act or other legislation than the General Data Protection Regulation, nor should such matters based on other legislation be taken into account as aggravating factors in the assessment of the administrative fine. In this regard, the Sanctions Board refers to the provisions of Article 83(5)(d) of the GDPR. According to the said provision, an administrative fine can be imposed for infringements of any obligations pursuant to Member State law adopted under Chapter IX of the GDPR. We also refer to the provisions of Article 88. Member States may provide for more specific rules by law to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context.
44. It should also be emphasized that Article 88 of the GDPR does not leave it to the discretion of the national legislator whether to limit the national regulations adopted based on the mentioned article outside the scope of administrative fines.
45. Article 83(7) of the GDPR stipulates how the scope of administrative fines may be limited by national legislation. There is no other national margin of discretion in relation to the scope of application of administrative fines.

The decision to impose an administrative fine has been made by the members of the Sanctions Board of the Office of the Data Protection Ombudsman.

Data Protection Ombudsman

[REDACTED]

[REDACTED]

Deputy Data Protection Ombudsman

[REDACTED]

[REDACTED]

Deputy Data Protection Ombudsman

[REDACTED]

[REDACTED]

Referendary Senior Officer

[REDACTED]

[REDACTED]



The document is signed electronically. The legitimacy of the signature can be verified at the registry of the Office of the Data Protection Ombudsman if necessary.

Additional information on this decision is available from the referendary

Senior Officer [REDACTED], telephone [REDACTED]

Applicable legal provisions

As set out in the grounds.

Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court pursuant to the provisions of the Administrative Judicial Procedure Act (808/2019). The appellate court is the Administrative Court of Helsinki.

Instructions for appeal are appended.

Service of notice

Notice of this decision will be served by post against an acknowledgment of receipt pursuant to section 60 of the Administrative Procedure Act (434/2003).

Appendices

Appeal instructions

Payment instructions for the administrative fine

Distribution

Complainant

[REDACTED]

Contact information of the Office of the Data Protection Ombudsman

Postal address: P. O. Box 800, FI-00531 Helsinki, Finland

Email: tietosuoja@om.fi

Telephone exchange: +358 (0)29 566 6700

Website: www.tietosuoja.fi

Office of the Data Protection Ombudsman

PL 800, FI-00521 Helsinki, Finland – tel. +358 29 566 6700 (exchange) – tietosuoja@om.fi – www.tietosuoja.fi



Notice: This document is an unofficial translation of the Data Protection Ombudsman's final decision (national record no. 1198/161/2022, IMI case no. 50199). Only the Finnish version of the decision is deemed authentic.

Record no. 1198/161/2022

IMI Case no. 50199

27 December 2022

Referring to complaints under national record numbers: 1875/452/2018, 2123/182/2018, 2405/182/2018, 3194/182/2018, 4318/146/2018, 1456/182/2019

Final decision of the Data Protection Ombudsman and the Collegial Body for Sanction

Case

Processing of personal data in connection with the [REDACTED] service

Controller

[REDACTED]

Case background

1. Between 22 May 2018 and 18 February 2019, five complaints concerning [REDACTED] (hereinafter: "█████" or "controller") were lodged in the Office of the Data Protection Ombudsman. Complaints concern [REDACTED] service (also: "█████" or "████").
2. During the abovementioned period, a complaint was lodged in the Austrian supervisory authority concerning the processing of personal data by the controller in [REDACTED] service. Given that the processing of personal data at issue has or is likely to have a significant effect on data subjects located in other Member States of the European Union, the matter must be processed in the cooperation mechanism according to Article 60 of the General Data Protection Regulation (hereinafter: "GDPR"). The Data Protection Ombudsman is deemed to be the lead supervisory authority regarding these personal data processing activities carried out by the controller. Hence the complaint lodged with the Austrian supervisory authority was transferred to the Office of the Data Protection Ombudsman on 18 July 2018. The case will be handled jointly with the other five complaints.
3. The Data Protection Ombudsman processes the complaints lodged by the complainants (hereinafter: also "complainants") jointly, on the basis of section 25 of the Administrative Procedure Act (434/2003).

Content of the complaints

4. According to the complaints, the use of a heart rate monitor manufactured by the controller requires the use of [REDACTED] service and acceptance of [REDACTED]'s Terms of Use and Privacy

Office of the Data Protection Ombudsman

P.O. Box 800, 00531 Helsinki, Finland – tel. +358 29 566 6700 (switchboard) – tietosuoja@om.fi – www.tietosuoja.fi



policy to which the complainants did not wish to consent. In order to use [REDACTED] service complainants must accept i.e., give their consent to the following processing operations:

- i. processing of personal data concerning the heart rate by ticking a box that states the following: "*I agree that [REDACTED] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [REDACTED] Privacy Notice. I can change my settings about this consent at any time.*";
- ii. transfer of personal data outside the EU/EEA by ticking a box that states the following: "*I agree that my personal data may be transferred and processed outside my country of origin as described in the [REDACTED] Privacy Notice. I can change my settings about this consent at any time.*"; and
- iii. [REDACTED]'s Terms of Use that state the following, among other things: *By saving, submitting, or transferring content to [REDACTED] services, you are granting [REDACTED] an uncompensated, global, transferable, sub-licensable right to use, reproduce, present in public, edit, translate, and share your User Content. Excluding the rights related to your personal data, the rights you have granted to [REDACTED] are irrevocable. Please note that even after you have closed your user account and your personal data has been deleted from [REDACTED] systems, material such as comments posted on discussion forums will not be removed. However, before closing your account, you can always remove User Content you have submitted to the services, including any comments posted.*"¹

Cross-border nature of the matter

5. [REDACTED] service is also offered in other EU/EEA Member States and the processing of personal data is subject to similar conditions, irrespective of the country in which the user is located. Since the processing of personal data which takes place in the context of the activities of a single establishment of a controller in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State, the case must be regarded as cross-border character within the meaning of Article 4(23) of the GDPR.
6. The case is therefore dealt within the context of a 'one-stop shop' mechanism in accordance with Article 60 of the GDPR.
7. According to an assessment of the matter, decisions concerning the purposes and means of the processing of personal data related to [REDACTED] are made in Finland, which is why the Office of the Data Protection Ombudsman is the leading supervisory authority referred to in Article 56 of the GDPR.
8. The Office of the Data Protection Ombudsman will deal with the matter in accordance with the procedure laid down in Article 60 of the GDPR in cooperation with the supervisory authorities of the participating Member States. In the present case, the concerned supervisory authorities (*hereinafter also: "CSAs"*) within the meaning of Article 4(22)(b) of the GDPR are the supervisory authorities of Italy, Belgium, the Czech Republic, France, Denmark, Greece, Germany, Hungary, Netherlands, Norway, Slovakia, Slovenia, Sweden, Luxembourg, Spain and Poland, since the processing affects or is likely to significantly affect data subjects in these Member States. The Austrian Supervisory Authority is a supervisory

¹ Extract from [REDACTED]'s Privacy Notice dated 22 May 2018



authority concerned on the basis of Article 4(22)(c) of the GDPR as it has received a complaint.

Proceedings in the cooperation mechanism

9. In accordance with Article 60(3) of the GDPR, the Office of the Data Protection Ombudsman as the lead supervisory authority, has provided relevant information on the matter to the CSAs.
10. The Office of the Data Protection Ombudsman has communicated controller's response to the CSAs². In addition, the Office of the Data Protection Ombudsman has reserved the CSAs an opportunity to present observations on written request for hearing of views and request for clarification before sending written request for hearing of views and request for clarification to the controller. Of the CSAs, the French Supervisory Authority (The Chair of the Commission Nationale de l'Informatique et des Libertés, *hereinafter: "CNIL"*) has provided comments to the Office of the Data Protection Ombudsman. The comments on written hearing concerned, *inter alia*, the following:
 - i. CNIL has drawn attention to the controller's response to the request for additional clarification 19.11.2019, in which the controller has stated that it processes information about the *length of the user, weight, age, training background, active orientation and sleeping goal*. CNIL has considered that it should be assessed whether the controller also processes other data belonging to special categories of personal data if it is able to combine the data collected. Also, CNIL has stated that information provided by the controller regarding the processing of special categories of personal data processed by the controller has not been clear.
 - ii. CNIL has also drawn attention to the processing of personal data concerning research and product development carried out by the controller.
11. As explained above, the Data Protection Ombudsman has already tried, before drafting a draft decision pursuant to Article 60(3) of the GDPR, to hear CSAs views on the preliminary assessment of the Data Protection Ombudsman.
12. The observations made by CNIL have been taken into account as follows:
 - i. Following the observation made by CNIL, a question has been added to written request for hearing of views and request for clarification on whether the controller processes other special categories of personal data.
 - ii. As the processing of personal data for research and product development purposes has not been the subject of complaints, the question concerning research and product development will not be dealt in the context of this decision. The case may be declared admissible on its own initiative at a later stage. In this context, the Data Protection Ombudsman notes that when registering for [REDACTED], it is currently possible to object to the processing of personal data for this purpose^{3,4}.

² Controller's response to the request for clarification 9 November 2018 and additional request for clarification 19 November 2019.

³ [REDACTED]'s website, visited on 1 May 2022

⁴ See also paragraph 101 of the decision



13. The draft decision of the Data Protection Ombudsman and the Collegial Body for Sanction has been submitted to the CSAs on 18 October 2022 in accordance with Article 60(3) of the GDPR. The CSAs has been required to submit a relevant and reasoned objection pursuant to Article 4(24) of the GDPR to the draft decision of the Data Protection Ombudsman and the Collegial Body for Sanctions by 18 November 2022.
14. On 18 November 2022 CNIL submitted a relevant and reasoned objection to the draft decision of the Data Protection Ombudsman and the Collegial Body for Sanctions. In its objection, CNIL is of the opinion that the Data Protection Ombudsman should exercise corrective powers provided for in Article 58(2) of the GDPR as a result of infringements of Article 7(2) and (4) of the GDPR⁵.
15. In addition to the objection, CNIL has submitted a comment on the draft decision. In its comment, CNIL proposes that the Data Protection Ombudsman associates its order under Article 58(2)(d) of the GDPR for the infringement of Article 9⁶ with a deadline the company must respect to comply with the GDPR.
16. The Data Protection Ombudsman has taken the objection raised by CNIL into account in its decision and added an order for infringement of Article 7 of the GDPR. The Data Protection Ombudsman has also taken into account the comment submitted by CNIL. Following the CNIL's objection, the amendments to the draft decision of the Data Protection Ombudsman were dealt with the Collegial Body for Sanctions on 8 December 2022.
17. None of the CSAs has within a period of two weeks expressed a relevant and reasoned objection to the revised draft decision. The deadline for objection has been 23 December 2022. Therefore, according to the Article 60(6) of the GDPR the lead supervisory and the CSAs are deemed to be in agreement with the revised draft decision and shall be bound by it.

Response received from the controller

18. The Office of the Data Protection Ombudsman requested clarification from the controller on 18 October 2019 and 4 November 2019. The controller submitted a response to the requests on 9 November 2018 and 19 November 2019. In its responses the controller submitted the following details, among others.

General information about [REDACTED]'s heart rate monitors and [REDACTED] service

19. The controller has provided the following general information about [REDACTED] service:

"The [REDACTED] service and [REDACTED]'s devices (wrist devices, sensors) are two separate things. When purchasing a [REDACTED] product, the customer does not automatically gain access to the [REDACTED] service. The majority of our devices require the use of the [REDACTED] service, some devices can be used completely or to some extent without the service. This information is shown on the packaging and in the instructions of devices. Information on the matter can also be found on our website.

One of the key principles with regard to [REDACTED]'s devices and services is that the devices (wrist devices and sensors) are used to collect data (e.g. heart rate, activity data and location data during sports activity) and the collected data is transferred to the [REDACTED] service for analysis in order to provide various added-value services. Although the basic functions of certain devices can be used

⁵ See paragraph 102 v of the decision

⁶ See paragraph 103 i of the decision



on their own, without the [REDACTED] service (so-called stand-alone use), use of the service is required in order to get the best added value.

The [REDACTED] service is free of charge but requires the user to sign up, accept the terms of use and give the required consent.

The complaints submitted to the Office of the Data Protection Ombudsman criticise the fact that a registered user must consent to [REDACTED]'s use of the customer's personal data and that the service promised when purchasing a [REDACTED] heart rate monitor cannot be used without giving this consent. However, the device and the service are in fact two separate things and the service is not "sold" in connection with the purchase. Instead, use of the service is recommended - and in some cases required. In the latter case (use of the product requires use of the service), the customer is informed about the service being required on the product packaging, among other places. However, there are separate terms of use for the service, which the customer must consent to before using the service. As stated above, we also offer customers who have purchased a device the opportunity to return the product if the customer is not ready to agree to the terms of the [REDACTED] service when creating a user account."

20. The controller has further specified [REDACTED] service as follows:

"The basic functions of the monitor include "setting the basic data of time and user (length, weight, date of birth, exercise background, activity target, sleeping goal). It is also possible to attach a separate heart rate sensor into the wrist device without [REDACTED] account. The basic functions include measuring the causes, activity and exercise with default profiles, such as running, walking and cycling. Depending on the activity, basic functions enable, for example, the measurement of heart rate, consumed calories, speed, training trips, tours and duration of the exercise. The device can also use timer and an alarm function. You can also change your user interface visually by selecting a lock-board of your choice. The amount of basic functions varies by type of equipment, and the properties of the device may enable, for example, breathing exercises.

In stand-alone use, the software of the device cannot be upgraded for the time being without the [REDACTED] code, but the device can be put into use and its basic functions can be used with the software installed on the device and that is available on the device when the customer buys the device. Of course, this software also includes all the functions available through the [REDACTED] service, but it is not possible to use them in stand-alone mode. These additional functions include various graphics and controls that require algorithms and platforms in the [REDACTED] service."

Consent as a legal basis for the processing of personal data

21. The controller has stated the following:

"In May 2018, along with many other companies, [REDACTED] also made changes to its legal documents due to the new data protection regulation. We rewrote documents, such as our Terms of Use and Privacy Notice, into a more user-friendly form. The actual Terms of use did not change much, and all changes were made for the advantage of the user."

22. The controller has stated that it has completely changed the grounds for processing due to the following factors:

"There were various reasons for changing the legal basis. The first reason was legislation outside the EU. As stated above, [REDACTED] is a global company with customers all over the world. Thus, [REDACTED] must also comply with the data protection laws of countries outside of the EU area. [REDACTED]

[REDACTED] At present, we can only offer the [REDACTED] service in one form (which is the same to everyone) around the world and can therefore not customise the principles related to the operation and use of the service on a country-specific



basis. We are currently looking into technical prospects for country-specific operation and use, which would take into account the unique features of each country and could help optimise this aspect of registration, but we are currently unable to offer such functionality.

[REDACTED] According to EU's interpretation, data based on heart rate combined with a user's other data (height, weight, age) is comparable to health data. This data can be used to draw conclusions on the person's health. Because the operation of the [REDACTED] service is largely based on the use of this type of data, we are directly compelled by law to use consent as the legal basis for collecting heart rate data from our customers.

The third reason for changing the legal basis was our desire to ensure that our customers truly understand the principles and practices used for processing their personal data. We wanted to make it clearer to our customers how we process their data. This primarily relates to customer service. We believe that some of our customers had not actually read our terms of use and privacy policy with sufficient care before agreeing to them, and we wanted to draw their attention to what is done to their data and how it is used. The submitted complaints have in fact shown that our concerns were well-founded. Nothing has changed in the actual processing of data."

23. In its response, the controller has described the collection of consent process as follows:

"Consent and new customers: When a new customer purchases a [REDACTED] device, the customer is instructed to sign up for the [REDACTED] service in order to gain full benefits from the device. However, use of the service is not mandatory and is not an automatic part of acquiring a device. If a new user does not wish to give the required forms of consent when registering into the [REDACTED] service, the customer can decide not to use the service and no data on the customer will be saved into [REDACTED]'s systems. No data on the customer is recorded into the [REDACTED] service before the customer has given the requested consents. If a customer decides to not agree to the terms of the [REDACTED] service and refuses to give the requested forms of consent, the customer is also entitled to return the device to the place of purchase and be refunded. However, it should be noted that, in accordance with our current policy, it must be possible to set up and use the basic functions of our wrist devices without signing up to the [REDACTED] service. Set up and use without the service is possible with devices such as devices brought to the market in the autumn of 2018 [REDACTED] and some devices that were already on the market.

Consent and old customers: When an old user first signed up to our service, the user agreed to our terms of use and privacy policy valid at the time of signing up. It was not possible to create a [REDACTED] without the acceptance of these documents. By agreeing to the terms, the user gave his/her consent to the collection of the user's data and any transfer of the data outside the EU/EEA. When [REDACTED] implemented changes to the legal basis for the processing of personal data, changing the basis from contract to consent, only the legal basis for processing sensitive data changed, not the actual processing of personal data. Thus, our old users have already given their consent to the same practices, only the legal basis has changed. If an old user does not wish to give his/her consent to these same practices on the new legal basis, we interpret this as the user having withdrawn his/her agreement to the Terms of use and Privacy policy which the user has previously agreed to, which in turn entitles us to terminate the user's contract and the use of the service. If a user does not wish to give his/her consent, the [REDACTED] account of the user will be locked and the user will have six months to change his/her mind, give his/her consent and continue the use of the service. After six months, the account and all data connected to it will be erased. For this entire six-month period, the user may exercise his/her legal right to transfer the data and may download the data using [REDACTED]'s account management service ([REDACTED]). A user may delete their own account or request the deletion of his/her account, in which case the account will be deleted within 30 days."



24. The controller further states the following:

"The controller is aware of the difficulties related to the use of consent in this respect and we did not decide upon it lightly. However, due to reasons related to countries outside the EU, we felt that we did not have any other option. And as stated above, the EU General Data Protection Regulation also requires us to ask for consent for the processing of our customers' heart rate data. We have made no changes to the processing of data itself and our old customers are not being forced to agree to anything they have not agreed to previously. This is in compliance with Article 7 of the GDPR, and customers always have the choice of whether or not they want to use our service."

25. In its response, the controller has referred to the decision (Decision 16 October 2018 Case Reference Number RFA0755227) issued by the UK Supervisory Authority (Information Commissioner's Office, hereinafter "ICO"). According to the controller, ICO has unambiguously stated in its decision that the controller's procedure complies with data protection obligations.
26. On 13 May 2022, the Office of the Data Protection Ombudsman requested the controller to submit the ICOs decision referred to in paragraph 25. The controller submitted ICO's decision on 20 May 2022.
27. ICO's decision to which the controller referred has concerned a complaint received by ICO in spring 2018. The complaint concerned the fact that the controller has required the complainant concerned to give their consent to the use of [REDACTED], even though the complainant has been a user of the [REDACTED] service for several years. As a result of the complaint, ICO has requested clarification from the controller.
28. In its clarification request, ICO has asked the controller to provide an explanation of why the controller has decided to request consent for the processing of personal data and what has led to a change in the grounds for processing. In addition, ICO has requested explanations as to why consent has also been required from old users whose personal data have already been processed by the data controller.
29. In the response submitted to ICO, the controller has told that when the GDPR became applicable, the biggest change in the controller's operations was changing the legal basis for processing from contract to consent. The controller has also been obliged to ask old users for consent to the processing of personal data, the transfer of data and the processing of sensitive personal data. The controller has explained that the processing of personal data in itself has not changed, but only old users have been asked to give their consent to the processing of personal data due to the requirements of the GDPR.
30. On 16 October 2018, ICO submitted a reply to the controller where ICO has stated that, in the light of the clarification provided by the controller, ICO welcomes the steps taken by the controller in relation to the change in the basis of processing based on consent and that the actions of the controller are in line with the GDPR. ICO has also stated that it does not consider it necessary to examine the controller's activities more extensively in terms of the grounds for processing.⁷

⁷ ICO's response of 16 October 2018: *"In light of the information you have provided, we are satisfied that [REDACTED]'s actions relating to the change in lawful basis for processing to account on consent, is in compliance with your data protection obligations. As such we do not request any further information from you, nor do we intend to take any further action in relation to the complaint raise by [REDACTED]."*



-
31. The Data Protection Ombudsman draws attention to the fact that the response submitted by the controller to ICO is equivalent to that provided by the controller to the Office of the Data Protection Ombudsman (see paragraphs 21 to 24 of this decision).

Disclosure of personal data to third parties

32. In its clarification, the controller states that the concepts "disclosure" and "transfer" are easily confused. On the disclosure of data, the controller stated the following:

"[REDACTED] never discloses the data to third parties. This is included in our Privacy Notice: [REDACTED] never discloses any of your personal information without a separate permission from you, unless it is necessary for handling your order, carrying out your request, or managing our interactive customer programs. Information may, however, be disclosed if necessary because of law, a court order, or a regulation or request issued by authorities."

Transfer of data outside the EU/EEA

33. With regard to the transfer of data, the controller has stated, among other things, the following:

"[REDACTED] transfers some data to outside the EU/EEA. Almost all [REDACTED] service user data is stored on servers located within the EU (Finland and Ireland). However, [REDACTED] does use a customer email service provider with a server located in the United States. We also use a service monitoring service provider with a server located in the United States. In both cases, it is possible that a user's email address or user ID is transferred to the service provider's server. These data storage locations have been the same as long as the [REDACTED] service has existed, and customers have been informed about data transfer in our Privacy Policy before May 2018 and in our Privacy Notice after May 2018.

Data transfer is subject to Article 49(1)a of the GDPR. In addition to the consent given by the user, we also adhere to safeguards put forward in Article 46. We conclude a data processing contract with every service provider we use. In order to ensure safe transfer and processing of data, we conclude a contract based on EU's standard contractual clauses with any service provider located outside the EU/EEA, located in a country that the EU deems to not have an adequate level of data protection or not certified with the EU-U.S. and Swiss-U.S. Privacy Shield.

Our customers, both old and new, have been informed about the transfer of data to outside their own country. We have used the same practice for the entire existence of the [REDACTED] service, and we have always informed our customers about this practice. We have noticed from customer contacts received by our customer service, that many of our customers have become more aware of the practice since we have started requesting a separate consent for data transfer. Increasing awareness has been one of our goals. According to our view, making our customers aware of the matter shows that our practice is in compliance with the GDPR. We help our customers to better understand what is done to their data. This seems to have come as a surprise to some of our customers, even though we have informed them about the practice before."

User content

34. The controller has provided, among other things, the following information about the user content:

"Content created by a user is always content published by the user in [REDACTED]'s services. User-created content is defined in our Terms of Use as follows: "In addition to the data transferred by you from [REDACTED] devices, you may also save or post on some of the [REDACTED] services content or other material that you have created yourself, such as images, videos, text, music, comments related to the data transferred from the devices, and data on your training sessions. You can also participate in discussion forums provided by [REDACTED] and post links on data related to your [REDACTED] account on provided social



media channels, or link your posts there. All the content you yourself have submitted, saved, or transferred to the services provided by [REDACTED] is hereinafter referred to as "User Content".

Content created by a user is not data uploaded from the user's device or information that the user provides when creating an account. Content created by a user is data which the user himself/herself chooses to share in group discussions or [REDACTED]'s social media channels, for example. Typical examples of content created by a user include videos or photographs from training sessions, events or competitions. The customer owns this material but [REDACTED] is allowed to use and share it. This data is material which the user himself/herself has published and the data does not come from the actual [REDACTED] service where the customer's personal data and training data is processed.

[REDACTED]

[REDACTED] [REDACTED]

In accordance with the Terms of Use, [REDACTED] may reuse such data published by a user. [REDACTED] does not interfere with content published by a user, except when the content is forbidden or inappropriate (e.g. racist, criminal or otherwise detrimental) in accordance with the Terms of Use.

[REDACTED] will not share any user content which the user has not shared himself/herself. Neither will [REDACTED] share training data shared by users in the [REDACTED]-service, for example. Any data that is reused/re-shared was originally published by the user, which means that the user has agreed to the sharing of the data."

Processing of personal data for research and product development purposes

35. In addition to complaints, the Office of the Data Protection Ombudsman has, on its own initiative, initiated to investigate the processing of research and product development described by the controller in its Privacy Notice. According to the response given by the controller, the controller processes the personal data of users on the basis of a legitimate interest for research and product development purposes. The data controller has also emphasised that the data is anonymous data. According to the controller:

"Only general data, such as age, gender, traineeship background, models of registered devices and applications used, will be included in the survey data. In addition to these, the research data will be connected to the training data provided by the equipment and synchronised in the [REDACTED] service. The data used will also be processed in such a way that individual data cannot be processed."

36. According to the controller, it has not been possible for the user to object to the processing of personal data for that purpose.

Written hearing of the complainants

37. According to section 34(2)(5) of the Administrative Procedure Act, the Office of the Data Protection Ombudsman has not requested the complainants to submit a response to the information provided by the controller, since the hearing of views is manifestly unnecessary.

Written request for hearing of views and request for further clarification

38. Due to the responses received in the matter, the Office of the Data Protection Ombudsman has sent to the controller the written request for hearing of views as referred to in section 34 of the Administrative Procedure Act. In the written request for hearing of views, the controller was reserved an opportunity to be heard, and to present an opinion on the facts of the case and the preliminary assessment made by the referendary of the Office of the Data Protection Ombudsman.



Facts of the case

39. The following facts are set out in written request for hearing of views.

General

40. When purchasing a data controller's heart rate device, the complainant does not automatically have access to [REDACTED] service. If the complainant wishes to use [REDACTED] service, it must accept the Terms of Use and Privacy Notice and give consent to the processing of personal data carried out by the controller. Consents are given by ticking the box indicating the consent. If the complainant does not wish to give consent to the processing of personal data carried out by the controller, the complainant will not have access to [REDACTED] service.

Consent to the processing of heart rate data

41. The controller requests explicit consent to the processing of special categories of personal data because the GDPR explicitly requires consent to be requested. Consent is also requested to improve data subjects' awareness of how the controller processes personal data.

42. [REDACTED] service is based on storing of data concerning the heart rate in [REDACTED] service. Thus, the use of [REDACTED] service requires a data subject to give consent to processing of data concerning the heart rate. If a customer who has purchased a heart rate device does not take [REDACTED] service in use but wishes to use the heart rate device in a stand-alone mode, no information on the heart rate is stored.

43. In order to take [REDACTED] service in use, the complainant must give consent by ticking the box that states "*I agree that [REDACTED] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [REDACTED] Privacy Notice. I can change my settings about this consent at any time.*" If the complainant does not give consent to the abovementioned, the complainant is unable to register for [REDACTED] service.

44. The abovementioned information provided by the controller implies that the controller processes data belonging to special categories of personal data other than only data concerning the heart rate. Information on the processing of special categories of personal data is provided in Privacy Notice as follows: "*The majority of [REDACTED]'s services are based on data collected on our products. Some of the collected data (e.g., heart rate data) are data where we always need your consent to collect and process. This consent is requested separately in each service where data belonging to groups of personal data requiring explicit consent is processed.⁸*"

45. In addition to the obligation to request consent for heart rate data under the GDPR, the controller also requests consent in order to improve the awareness of the processing of personal data by the controller.

Consent to the transfer of personal data to third countries

46. In order to be able to register with [REDACTED] service, users must give their consent to the transfer of their data outside the EU/EEA. The controller has told that it transfers personal

⁸ Extract provided by [REDACTED] from the data protection practice on its website on 17 October 2018



data under the EU-U.S. and Swiss-U.S. Privacy Shield. In countries where the Privacy Shield arrangement does not apply and the Commission has not valued an adequate level of data protection, the data has been transferred by the controller under the standard contractual clauses. The controller's grounds for transfer of personal data are also Article 49(1)(a) GDPR, i.e., explicit consent.

47. In its response, the controller has reported that it has transferred personal data outside the EU/EEA to the United States. No other third countries have been identified in the response. Thus, the Office of the Data Protection Ombudsman will only assess the transfer of data in respect of the United States.
48. The controller has informed that it requests consent to the transfer of data also because it considers that the data subjects are thus more aware of the processing of personal data carried out by the controller.

Consent to the “user content”

49. The controller requests a data subject to accept the Terms of Use which states: “*When storing, sending or transferring content to [REDACTED]’s services, you give [REDACTED] an unconditional, global, transferable and relicitable right to use, copy, present, edit, translate and share your own content created by the User. Except as regards your personal data, rights given to [REDACTED] cannot be revoked.* [--]. “User content” is not data from the user’s device or data provided by the user’s account when creating an account, but “content” created by the user refers to information that the user chooses to share, for example in group discussions or through the controller’s social media channels.
50. If the complainant does not accept the Terms of Use, the complainant does not get access to [REDACTED] service. The controller requests the user to accept the Terms of Use in order to make users more aware of the principles and practices related to the processing of personal data.

**

51. In the written request of hearing of views, the Office of the Data Protection Ombudsman has requested additional clarification. The controller was requested to provide additional information on whether it is processing other personal data concerning health belonging to special categories of personal data. In the written hearing⁹, the referendary has stated that if the controller processes other personal data belonging to special categories of personal data in addition to the heart rate data, according to the referendary’s preliminary assessment, the controller has not had data subject’s consent to process other personal data concerning health in accordance with the GDPR. In its response to request for additional clarification, the controller has stated that it also processes the maximum oxygen uptake and the body mass index. In the written request of hearing of views, it has been noted that if the controller processes other data concerning health in addition to a heart rate data, the controller has not had a consent to the processing of such data.

⁹ Under “Sanction to be proposed”



52. In the written request for hearing of views, the controller has been asked to provide clarification on the following:

- I. Does the controller process data of health other than those obtained by combining the user's age, length, weight and heart rate? Please indicate which user data the controller combines and which data belonging to special categories of personal data is being processed.
- II. The controller has told that it is processing data in order to generate value for customers. Are there other purposes for the processing of heart rate data than the abovementioned?
- III. According to the data Privacy Notice and response to additional clarifcation, data subjects have not been able to object to the processing of the data for research and product development purposes. Has the controller changed the procedure in this regard? If yes, when has the procedure changed and how has it been implemented?
- IV. How many registered persons have logged in to [REDACTED] service and thus gave their consent to the Terms of Use between 25 May 2018 and 18 February 2019? If the exact number cannot be given, we kindly ask you to provide an estimate of the number.

Controller's response to written request for hearing of views

53. As explained above, the controller has been given an opportunity to express an opinion on the referendary's preliminary assessment and the facts of the case presented in written request for hearing of views.
54. The controller has been given an opportunity to provide information on requirements and information that may have an impact on the decision-making in the matter. Also, the controller has been given the opportunity to highlight circumstances referred to in Article 83(2) of the GDPR which, in the controller's view, should be taken into account when deciding and imposing any administrative fine.
55. The controller submitted a response to written request for hearing of views on 14 January 2022. In its response the controller states, inter alia, the following.

General

56. The data controller has not been able to bring to production all the reforms it has planned that improve data protection. However, the controller says that it is investing in the development of information security and data protection. The controller states that it has made changes to prioritise a number of development projects in the area of operation, which aim, among other things, to promote identified deficiencies in the data protection practices of [REDACTED] service, for example.

57. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



58. The controller reports that there are millions of users in [REDACTED] service. In [REDACTED], personal data are currently equal regardless of the user's location. An effort has been made to draft [REDACTED]'s Privacy Notice in such a way that it would meet the requirements of many different countries. According to the controller, the data protection practice related to the service has been published in 28 language versions and a total of 49 different country and language combinations have been published.

59. The controller states that the heart rate monitor is a device that measures the frequency of the heart beating. Heart rate monitor can be a transmitter surrounded by the chest or a receiver that is attached to the wrist and resembles watch. [REDACTED]

[REDACTED] As a rule, the basis for measuring a heart rate is the level of activity of the user, but there are other factors contributing to it.

Transfer of personal data

60. The data controller states that it is an international company operating in the global market, and there are different data protection provisions in its different markets. The controller states that it has explored the possibility of localising the service platform, but it has not been possible with the technology in use. In the current situation, the controller provides an equal version of its services to all areas. According to the controller, requesting country-specific consents is particularly challenging because the country information provided by the user is not reliable. In alphabetical countries, the first country is well over-represented, which suggests that the user's registration does not always complete the correct information. In the controller's view, this is a common problem in online services that do not require strong customer authentication (e.g. bank identification) that cannot even be implemented globally.

User content

61. Between 25 May 2018 and 18 February 2019 [REDACTED] service has, according to the controller, included activities that rely on "user content". Users have been able to share their sports performance with followers managed by them in the [REDACTED]-view, where it has been possible to discuss the results. [REDACTED]-function has included groups, events and clubs where users have been able to discuss with other users in the same group or event and share training information for them. [REDACTED]-function is intended for [REDACTED] users who train in sports centres that use the [REDACTED] service. [REDACTED]-function also shows the sports centre's own [REDACTED], where the customers using [REDACTED] service of the sports centre have been able to share their exercises accordingly and discuss with other clients who use [REDACTED] service of the sports centre.

62. Sharing "user content" on platforms and discussion forums provided by the controller has been voluntary for the user. The user has also been able to choose to keep their profile private, in which case the information has not been visible to other users. Therefore, consent to the processing of the data has been necessary to allow the user to use [REDACTED] service of which the functions in question were an integral part. When creating their account, the user has read the Terms of Use and Privacy Notice and has given their consent to the following: *"I agree that [REDACTED] can collect and process my personal data in the manner described in [REDACTED]'s Privacy Notice. I can amend the settings related to this consent at any time."*



63. The controller has closed down [REDACTED]-view and [REDACTED]-function on 19 January 2021. [REDACTED]-function is still in use with regard to content other than that shared by the user, for example in order to register for lessons at sports centres.

Controller's response to question I presented in the written request for hearing of views and request for additional clarification

64. The controller states that it does not process other data belonging to special categories of personal data in addition to the heart rate data.
65. According to the controller, it is not possible to draw any direct conclusions on a person's health other than synthesis data (raw) data or derived data collected by the controller. Some abnormality collected may be typical of specific diseases or health problems, but in the controller's view, in order to make conclusion regarding health, additional data which are not processed by the controller would be needed. The controller is of the opinion that it is generally known that significant overweight (body mass index) or low physical activity can increase the risk of multiple diseases or be associated with health problems. However, this is not automatically the case and, in the view of the controller, a person's health cannot be inferred from the body mass index or activity alone.
66. The controller states that based on user's heart rate and acceleration data the controller calculates sleeping data of which the user might notice that they have slept poorly. However, according to the controller, sleeping data cannot be used to determine the causes of poor sleep. The reason may also be related to external disruptive factors. Therefore, in order to conclude on the state of health, additional information is required of which the controller does not process.
67. The controller states that the data collected by the data controller is rather wellbeing data that the user can use when analysing their own well-being and when making changes that support it in life. It is only with the help of additional information, any medical examinations and healthcare professionals that the user can draw conclusions about their health. According to the controller, the devices manufactured by the controller are also not medical devices or meet the criteria for their approval.
68. The data collected by the controller consists of information provided by the user itself and of data collected using devices. The profile information provided by the user are gender, age, length, weight, VO2 max, maximum heart rate, resting heart rate, aerobic and anaerobic threshold, aerobic maximum speed MAS, aerobic maximum power MAP, aerobic maximum power (MAP), functional threshold efficiency FTP, target sleep time and daily activity target.
69. The user's body mass index is calculated on the basis of length and weight. In addition, the controller collects heart rate, acceleration and location data as a raw data. From this data, the controller calculates the data derived with the help of its algorithms and presents it to the user in [REDACTED] service. It is not possible to directly draw conclusions about the person's health from the (raw) data collected by the controller or the derived information calculated with algorithms

Controller's response to the question II presented in the written request for hearing of views and request for additional clarification

70. In addition, according to the controller, data concerning heart rate are processed for research and product development purposes, which play a very important role in the further



development of algorithms and services. The legal basis for processing is either a legitimate interest or, in the case of separate research projects, consent of the data subject.

Controller's response to the question III presented in the written request for hearing of views and request for additional clarification

71. According to the controller, the implementation of the objection is currently under way. [REDACTED]

[REDACTED] The technical planning of the objection function is scheduled for the first possible date for the first annual Quartet of 2022. Resources have been reserved for technical implementation for the next annual quartet.

Controller's response to the question IV presented in the written request for hearing of views and request for additional clarification

72. The number of users who have approved the Terms of Use between 25 May 2018 and 18 February 2019 is 3.47 million. The controller states that they have renewed their Privacy Notice and Terms of Use on 15 May 2018, which means that during the abovementioned period most of the old users have also accepted the updated terms and conditions. New customers share of the number is 1.18 million.

On the applicable legislation

73. The GDPR has been applied since 25 May 2018. As an EU Regulation, the GDPR is legislation directly applicable in the Member States.
74. Complaints were lodged to the Office of the Data Protection Ombudsman between 22 May 2018 and 18 February 2019. A complaint has also been lodged with the Austrian Supervisory Authority during the abovementioned period.
75. In EU law, a key principle is the principle of legal certainty. A ban on the application of retroactive legislation has been derived from this principle in several decisions of the Court of Justice of the European Union. Under that prohibition, EU law does not, as a general rule, have retroactive effect.
76. In this respect, legal practice recognises two types of retroactivity: true retroactivity and material retroactivity. "True retroactivity" means application of new legislation to sets of facts that have been fully realised during old legislation. In principle, such true retroactivity is prohibited in the legal practice of the Court of Justice of the European Union.
77. "Material retroactivity" refers to application of new legislation with effects directed at the future in a situation that arose while earlier legislation was in force, and the legally relevant activity continues under the new legislation. The Court of Justice of the European Union has accepted such material retroactivity. The Court has stated that legislation on EU law must be deemed to reach legal effects upon entry into force even when the new legislation specifies consequences of states of matters that commenced during the old legislation. When evaluating the permissibility of retroactive legislation, the Court has also paid attention to private legal subjects' need for legal protection.



78. As said, the complaints were lodged with the Office of the Data Protection Ombudsman between 22 May 2018 and 18 February 2019, i.e., both before and after application of the GDPR commenced. In the case at hand, activity subject to complaint continued after application of the GDPR had begun, and this is why the GDPR is applied to the processing of the matter.

The applicable legislation

79. Pursuant 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.
80. Pursuant to Article 4(11) of the GDPR, '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.
81. Pursuant to Article 4(15) of the GDPR 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. Pursuant to recital 35 of the GDPR, personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject.
82. Pursuant to Article 4(22) of the GDPR 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:
(a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
(c) a complaint has been lodged with that supervisory authority.
83. Pursuant to Article 4(23)(b) of the GDPR 'cross-border processing' means 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.
84. Pursuant to Article 4(24) of the GDPR 'relevant and reasoned objection' means an objection to a draft decision as to whether there is an infringement of this Regulation, or whether envisaged action in relation to the controller or processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the Union.
85. Pursuant to Article 5(1)a of the GDPR personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency").



-
86. Pursuant to Article 6(1)(a) of the GDPR states that processing shall be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.
 87. Pursuant to Article 7(2) of the GDPR, if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. Under paragraph 4 of the same Article, when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.
 88. Pursuant to Article 9(1) of the GDPR states that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. Under paragraph 2 of the same Article, paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
 89. Pursuant to Article 13(1)(c) of the GDPR states 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 the information under Article 13 of the GDPR.
 90. Pursuant to Article 49(1) of the GDPR, in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
 91. Pursuant to the Article 58(2)(b) of the GDPR each supervisory authority shall have a corrective power to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR.
 92. Pursuant to the Article 58(2)(d) of the GDPR each supervisory authority shall have a corrective power to order the controller or processor to bring processing operations into compliance with the provisions of the GDOR, where appropriate, in a specified manner and within a specified period.
 93. Pursuant to the Article 58(2)(i) of the GDPR each supervisory authority shall have a corrective power to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.
 94. Pursuant to the Article 60(1) of the GDPR 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.

95. Pursuant to the Article 60(3) of the GDPR 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.
96. Pursuant to the Article 60(4) of the GDPR 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.
97. Pursuant to the Article 60(5) of the GDPR 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.
98. Pursuant to the Article 60(6) of the GDPR 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.

Judicial question

99. As presented above, the Data Protection Ombudsman shall review and decide on the case based on the GDPR and the Data Protection Act. The following judicial questions need to be resolved in this case:
 - i. Whether the controller has been obliged to request consent to the processing of heart rate data;
 - ii. Whether the controller has been obliged to inform about the processing of personal data related to [REDACTED] service when purchasing a heart rate device in accordance with Article 13 of the GDPR;
 - iii. In addition to a heart rate data, whether the controller is processing also other data belonging to a special categories of personal data concerning health. Where the controller also processes other health data belonging to special categories of personal data, the consent requested by the controller to the processing of such data has not been specific and informed as in Article 4(11) of the GDPR;
 - iv. Whether the controller has had grounds for the transfer of data to third countries; and
 - v. Whether the consent collected by the controller to the processing of user content been in compliance with the GDPR?



100. If the processing of personal data by the controller has not been in compliance with the provisions of the GDPR, the Data Protection Ombudsman will assess if it should apply the corrective powers bestowed on to it under Article 58(2) of the GDPR.
101. Complaints lodged to the Office of the Data Protection Ombudsman or to the Austrian Supervisory Authority did not concern a processing operation concerning research and product development. In order to speed up the processing of these complaints, the Data Protection Ombudsman will, in this case, exclude from the decision question concerning the processing of personal data for the purposes of research and product development that has been considered *ex officio*.

Decision and grounds of the Data Protection Ombudsman

Decision

102. The Data Protection ombudsman takes the following view:
- i. The controller has been obliged to request explicit consent to the processing of heart rate data on the basis of Article 9(2)(a) of the GDPR.
 - ii. The controller has not been obliged to inform about the processing of personal data in [REDACTED] in accordance with Article 13 of the GDPR when purchasing a heart rate device.
 - iii. In addition to the heart rate data, the controller also processes other data concerning the health of the data subject, when the controller is processing maximum oxygen uptake and the body mass index. The consent requested by the controller to the processing of other data concerning health has not been in compliance with the GDPR, and therefore the controller has not had a legal basis for processing other health-related data in accordance with Article 9(2) of the GDPR.
 - iv. At the time when the complaints were lodged, the controller had grounds to transfer data to United States.
 - v. The consent collected by the controller to the processing of user content did not comply with Article 4(11) of the GDPR and it did not meet the conditions for consent laid down in Article 7(2) and (4) of the GDPR.

Order

103. Pursuant to Article 58(2)(d) of the GDPR, the Data Protection Ombudsman shall order the controller:
- i. to bring the consent collected for the processing of maximum oxygen uptake and the body mass index into compliance with the GDPR within three months for new data subjects, and within six months for existing data subjects from the date of receipt of the decision;
 - ii. to assess whether, in addition to heart rate data, maximum oxygen uptake and the body mass index, it processes other health data belonging to special categories of personal data when combining user-related data in [REDACTED] service. Where the controller processes data belonging to special categories



of personal data, the controller must ensure that it has consent under the GDPR to the processing of all data relating to health that it processes in the context of [REDACTED] service; and

- iii. to ensure, without delay of the date of receipt of the decision that the controller has a legal basis pursuant to Article 6(1) of the GDPR to process personal data in connection with "user content".

Reprimand

104. The Data Protection Ombudsman issues a reprimand to the controller under Article 58(2)(b) of the GDPR, as the consent requested by the controller to process the maximum oxygen uptake and the body mass index has not been in line with the GDPR.

Administrative fine

105. The controller has not had a legal basis in accordance with the requirements of the GDPR for the processing of personal data that are an integral part of the controller's core business activity, which can be considered to include the processing of data concerning health.

106. Therefore, the Data Protection Ombudsman considers that deciding whether the reprimand under Article 58(2)(b) of the GDPR constitutes a sufficient sanction for the controller's infringement regarding consent that is not in line with the GDPR should be subject to the assessment of the Collegial Body for Sanctions.

107. According to section 24 of the Data Protection Act, the administrative fine provided for in Article 83 of the GDPR is imposed by the Collegial Body for Sanctions formed jointly by the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen. To the extent that the consent concerning maximum oxygen uptake and the body mass index collected by the controller has not been in compliance with the GDPR, the matter is referred to the Collegial Body for Sanctions. The Collegial Body for Sanctions must therefore assess whether an administrative fine under Article 58(2)(i) of the GDPR is to be imposed on the controller in addition to the reprimand and orders issued by the Data Protection Ombudsman.

Grounds

Consent to the processing of heart rate data

108. In order to register for [REDACTED] service, the controller has required the complainants to give consent to the following: "*I agree that [REDACTED] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [REDACTED] Privacy Notice. I can change my settings about this consent at any time.*" In a complaint lodged in the Office of the Data Protection Ombudsman, the complainant has



questioned the activities of the controller, as when joining [REDACTED] service, the complainant had to give consent to the processing of the heart rate data.

109. According to the controller, [REDACTED] contains information on the maximum heart rate and resting heart rate. In the annex to the letter sent to the European Commission by the Working Party WP29¹⁰, the Working Party considered that health data should, in a broad interpretation, concern the heart rate data measured by an application regardless of whether it is performed by medical professional or by devices and apps freely available on the commercial market and irrespective whether these devices are marketed as medical devices or not.
110. The Working Party has also considered that it is not possible to draw conclusions about a person's current or future state of health by means of an individual's registration, which includes information on the person's weight and heart rate data. The Working Party is of the opinion that in addition to the abovementioned data, at least information on the person's age or gender would be needed. In the view of the Working Party, if data on weight and heart rate were to be collected over a longer period of time and such data could be combined with data on a person's age or sex, conclusions could be drawn from the health of the data subject.
111. In [REDACTED] service, the controller processes information on a person's age, gender, weight, maximum and resting heart rate. On the basis of the above, the Data Protection Ombudsman considers that the heart rate data combined with other data processed by the controller reveals information on the data subject's health. Therefore, heart rate data must be regarded as data concerning health within the meaning of Article 4(15) of the GDPR, and thus the controller processes personal data belonging to special categories of personal data in accordance with Article 9(1) of the GDPR.
112. According to Article 6 of the GDPR, there must be a legal basis for processing personal data. Where the personal data processed are data concerning health, the controller must have a legal basis for processing such data in accordance with Article 9(2) of the GDPR. In the present case, since the controller processes heart rate data in order to produce an added value service, the data subject must give the explicit consent to the processing of heart rate data. Therefore, the controller has been obliged to request for consent to the processing of data concerning heart rate.
113. The complaints lodged in the Office of the Data Protection Ombudsman have not concerned whether the requested consent to the processing of heart rate data complies with the GDPR. Instead, it has been questioned whether the controller should request consent to the processing of heart rate data.

Information on the processing of personal data

¹⁰The Working Party on Data Protection WP29 has sent a letter to the European Commission, including annexes, clarifying the concept of health data for lifestyle and well-being applications. https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf



-
114. In complaints lodged to the Office of the Data Protection Ombudsman, the complainants considered that they had been forced to register to [REDACTED] service and thus to accept the processing of personal data in [REDACTED] service in order to use the heart rate watch.
115. The controller has reported that [REDACTED] service and its equipment (e.g., heart rate device) are two separate things. The controller's heart rate device and its basic functions can be used without [REDACTED] service. The basic functions of certain devices include measuring the heart rate, activity and exercise with default profiles, such as running, walking and cycling. Depending on the activity, basic functions enable, for example, the measurement of heart rate, consumed calories, speed, training trips, tours and duration of the exercise. However, in order to gain added value service, i.e. the utilisation of algorithms, the use of [REDACTED] service is required. Therefore, the customer is not tied to the use of [REDACTED], even though the [REDACTED] service is necessary for obtaining an added value service.
116. The controller states that if the device in question requires the use of [REDACTED] service in order to gain an added value service, information regarding this requirement can be found in its device package and in its Terms of Use. According to the controller, the customer also has right to return a device that they have purchased if they do not want to use [REDACTED] service. It is not within the jurisdiction of the Office of the Data Protection Ombudsman to assess whether a product or service meets the legitimate expectations of the consumer. It is within the jurisdiction of the Office of the Data Protection Ombudsman to assess whether information on the processing of personal data has been provided in a just-in-time as required by the GDPR.
117. The basic functions of the [REDACTED]'s heart rate watch are available without [REDACTED] service. Therefore, a data subject must be provided with the information before the use of the service, i.e., prior to registration in [REDACTED] service.
118. According to a complaint lodged in the Office of the Data Protection Ombudsman, the complainant states that they have been surprised to the fact that they had to take [REDACTED] service in use. However, as stated above, the heart rate device and its basic functions can be used without [REDACTED] service. In this context, the Data Protection Ombudsman also draws attention to the fact that, according to the controller, the data controller informs the use of [REDACTED] service in its device package and the customer also has right to return the device.
119. In accordance with Article 13 of the GDPR, information on the processing of personal data must be provided when personal data are collected from a data subject. The Data Protection Ombudsman considers that the controller must thus inform the data subject about the processing of personal data prior to the collection of personal data, i.e. when entering or registering into the service. When joining [REDACTED], customers will be able to familiarise themselves with the Terms of Use and Privacy Notice. In particular, the Data Protection Ombudsman draws attention to the fact that the basic functions of the heart rate device can also be used without [REDACTED] service, which is why, in the opinion of the Data Protection Ombudsman, [REDACTED] is not that integral part of the heart rate device that the controller's information on the processing of



personal data should not be considered sufficient in the present case. Similarly, the Data Protection Ombudsman considers that the controller's information on the processing of personal data has been transparent in accordance with Article 5(1)(a) of the GDPR.

Consent to the processing of other health data

120. As a preliminary point, the Data Protection Ombudsman draws attention to the fact that the controller's information on the processing of specific categories of personal data other than heart rate data given at the time of the registration is incompatible with the information provided by the controller in its response to the request for clarification.
121. When registering for [REDACTED] service, the controller informs the following: "*I agree that [REDACTED] may collect and process my sensitive personal data such as heart rate and other health data considered as sensitive data as described in the [REDACTED] Privacy Notice. I can change my settings about this consent at any time.*"
122. The Data Protection Ombudsman therefore considers that the purpose of the controller has been to seek the consent of the data subject by an act expressing consent to the processing of *other health data considered as sensitive data*.
123. However, in the response submitted to the Office of the Data Protection Ombudsman, the controller has presented that it does not process other data belonging to special categories of personal data other than data relating to heart rate.
124. The Data Protection Ombudsman will firstly assess whether, in addition to heart rate data, the controller processes other health data belonging to special categories of personal data and, secondly, whether the abovementioned practice of requesting consent for the processing of other specific categories of personal data fulfils the conditions for consent.

Processing of health-related data in [REDACTED] service

125. According to the response given by the controller, the data collected by the controller consists of data provided by the user themselves and of data collected with the help of devices. The profile information provided by the user is gender, age, length, weight, VO2max (maximal oxygen uptake), maximum heart rate, resting heart rate, aerobic and anaerobic threshold, aerobic maximum speed of MAS, aerobic maximum power MAP, functional threshold power FTP, target time of sleep and daily activity target.
126. The data controller has presented that it is not possible to draw any direct conclusions about a person's state of health other than heart rate, and therefore the controller, is in a position that it does not process other data concerning health. According to the controller, in order to draw conclusions about health, the controller would also need data that it does not process. The controller has considered that it is only with the help of additional information, any medical examinations and healthcare professionals that the user can draw conclusions about their health from the data collected by the data controller.



127. The controller has also considered that its devices are not medical devices or do not meet the criteria of such devices. In this context, the Data Protection Ombudsman refers to the view expressed by the Working Party on the first judicial question presented above, that the fact whether or not the device has been marketed as medical devices is irrelevant when assessing whether the data should be concerned as health data.

128. According to the Annex to the letter of the Working Party, data collected through lifestyle applications and devices should not, in general, be regarded as health-related data within the meaning of Article¹¹ 8 of the Personal Data Directive. The application of the GDPR has not changed the definition of health data. The Working Party's view concerns the so-called raw data, on which it is not reasonable to draw conclusions about the state of a person's health. Thus, not all information obtained from applications or devices is information about a person's health. Taking into account the wording of Article 4(15) of the GDPR "*personal data related to the health revealing his or her state of health [--]*", the Data Protection Ombudsman also considers that a single data collected by the controller does not necessarily reveal a person's state of health.

129. An example of so-called raw data given by the Working Party is the amount of steps taken by the data subject during the day, which would not be combined with other data collected about the registered user. The Working Party has also considered that the so-called raw data may, however, become health-related data when the data can be used to determine a person's state of health. Thus, the intended use of so-called raw data must be taken into account when assessing whether the data is health-related data referred in the GDPR.¹² The results of the combination of data and the purpose of the controller should also be taken into account.

130. In its guidance on the processing of health data for scientific research purposes in the context of the COVID-19 outbreak, the EDPB¹³ has considered that health data can be derived from different sources, for example data may become health data by cross referencing with other data thus revealing the state of health or health risks. With regard to the concept of health data, the EDPB referred to the judgment *Bodil Lindqvist* (C-101/01¹⁴) of which, in paragraph 50, the Court held that the term 'data concerning health' in Article 8 of the Personal Data Directive must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the

¹¹ Personal Data Directive repealed by the General Data Protection Regulation

¹² The Working Party on Data Protection WP29 has sent a letter to the European Commission, including annexes, clarifying the concept of health information for lifestyle and well-being applications. Attachment to the letter: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

¹³ Guidelines 03/2020 on the processing of data concerning health for the purposes of scientific research in the context of the COVID-19 Outbreak, p. 5 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

¹⁴ Judgment of the Court on 6.11.2003 in Case C101-01 Göta hövrät v Bodil Lindqvist <https://curia.europa.eu/juris/showPdf.jsf;jsessionid=A04867935AB30679DC72F953B32203C0?text=&docid=48382&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=2610677>



health of an individual. As mentioned above, the GDPR has not changed the definition of health data.

131. It should also be noted that, under the joint guidance of the National Supervisory Authority for Welfare and Health and the Office of the Data Protection Ombudsman (30.11.2017, record no. 2810/41/2017), the Data Protection Ombudsman stated that lifestyle data is part of a broader concept of health data¹⁵.
132. The controller has reported that it collects raw data from devices, from which it calculates data derived from its algorithms and presents to the user in [REDACTED]. In [REDACTED] service, users can see, for example, the heart rate zones during their sports activities; heartbeat (maximum and minimum) as well as calories consumed. The user will also be able to review its performance in the longer period of time. It is possible for the user to view information on their activity and sports performances by means of reports drawn up by the controller. As explained above, the controller combines the data collected on the user in order to provide the user with information on the user's activity and wellbeing as described above.
133. The Data Protection Ombudsman further highlights that not all single data should be considered data concerning health. However, if the controller will combine single data with other single data, and these combined data make it possible for the controller to draw conclusions about a person's current or future state of health, the processing of the single data may result that this data in question should be considered to be health data within the meaning of Article 4(15) of the GDPR and thus as data belonging to special categories of personal data in accordance with Article 9 of the GDPR.
134. The controller has reported that it is processing information on maximum oxygen uptake (VO2max). The controller states on its website that *OwnIndex* resulting from the [REDACTED] fitness test is comparable to maximum oxygen uptake (VO2max), which is commonly used as an indicator of aerobic fitness. According to the controller's website, the aerobic condition is related to how well the circulatory system is capable of transmitting oxygen to the body. The better aerobic condition, the stronger and more effective the heart. Good aerobic condition, among other things, reduces the risk of high blood pressure and reduces the risk of developing cardiovascular diseases or stroke.¹⁶
135. The controller has thus also recognized that the maximum oxygen uptake indicates the ability of the circulating system to transmit oxygen to the body and that the maximum oxygen uptake is thus linked to different diseases. The Data Protection Ombudsman considers that the information on the user's maximum oxygen uptake (VO2max, combined with an identifiable natural person, also indicates the person's state of health, which is why, considering the views of the Working Party and the broad interpretation of health data, the Data Protection Ombudsman considers that the maximum oxygen

¹⁵ The guidance provided by the Office of the Data Protection Ombudsman and the National Supervisory Authority for Welfare and Health (Valvira) has concerned the transfer of samples and related information to the biobank under the Biobank Act. [Data Protection Ombudsman 30.11.2017 – FINLEX ®](#)

¹⁶ [REDACTED]



uptake should be regarded as data concerning health within the meaning of Article 4(15) of the GDPR. In its assessment, the Data Protection Ombudsman has also noted that the controller can draw the above conclusions on the basis of the data it processes.

136. The controller has also stated in its response that the length and weight of the data subject is used to calculate the user's body mass index. The body mass index processed by the controller shall also be considered as data concerning health within the meaning of Article 4(15) of the GDPR.
137. In other respects, the Data Protection Ombudsman does not assess which other data concerning health is processed by the controller but leaves it to the controller's responsibility.
138. The Data Protection Ombudsman is of the opinion that the controller can and explicitly its purpose is to combine user's data in [REDACTED] in order to provide the data subject information regarding its activity with the help of algorithms. Similarly, even if the controller does not intend to directly process data concerning the health of data subjects, the Data Protection Ombudsman considers that the controller *de facto*, by combining data relating to a registered user, processes data concerning health in [REDACTED] service.
139. The Data Protection Ombudsman pays particular attention to the fact that the data controller has reported that the data it has collected is welfare data that users can use when analyzing their own well-being and making changes that support it in their lives.

Consent to the processing of other health data belonging to special categories of personal data

140. Based on the grounds presented in more detail above, the Data Protection Ombudsman has considered that, in addition to heart rate data, the controller processes at least the maximal oxygen uptake and the body mass index, i.e., also other health data belonging to special categories of personal data. According to Article 9(1) of the GDPR, the processing of such data is, in principle, prohibited. However, data concerning health may be processed, for example, on the basis of explicit consent by the data subject (Article 9(2)(a) of the GDPR).
141. The Data Protection Ombudsman notes that the purpose of the controller has been to request consent for the processing of other health related data by means of an act indicating consent, as the controller has requested consent as follows: I agree that [REDACTED] may collect and process my sensitive personal data, such as heart rate *and other health data considered as sensitive data* in the manner described in the controller's Privacy Notice.
142. According to Article 4(11) of the GDPR, consent must be, *inter alia*, specific and informed. Specific consent means consent requested for "one or more specific purposes". Specific consent therefore means that the data subject is expressly informed of the intended purposes for the use of data relating to them. In the EDPB Guidelines on Consent, the EDPB has stated that in each request for consent, the controller should *describe which data will be*



processed for each purpose¹⁷. For consent to be informed, data subjects must also be informed of the type or types of data collected and used¹⁸.

143. Moreover, the processing of personal data belonging to special categories of personal data requires that consent is *explicit* in accordance with Article 9(2)(a) of the GDPR.

144. In its Privacy Notice, the controller informs that it is processing personal data for the purposes listed in the Privacy Policy. In the Privacy Notice, the controller informs, among other things, of the following:

"When you create a user account for [REDACTED] services, we ask for some personal information (for example your name, email address, gender and age). We need this information in order to provide you with a personalized experience with our services. For example, we use your age info to give you a more accurate calculation of burnt calories."

[REDACTED] is a free fitness and training app and web service that helps you track your training, activity and sleep data as well as analyze your progress. It works together with your [REDACTED] product and acts as your automatic training diary: all your training, activity and sleep data syncs from your product to your [REDACTED] account."

145. The Data Protection Ombudsman considers that the controller *per se* informs the data subjects of the processing of their personal data for purposes such as the analysis of activity and training. However, the controller does not inform the data subjects of the types of personal data processed and of the purposes for which each type of personal data is being processed.

146. The Data Protection Ombudsman notes that the controller has, in its response to the Office of the Data Protection Ombudsman, listed data it processes. However, the same information has not been provided with the data subject at the time when the controller has requested the data subjects consent.

147. Since the controller has not provided information with the data subject on the purposes and types of data its processing, the consent requested by the controller to the processing of other health data cannot be considered as consent within the meaning of Article 4(11) of the GDPR.

148. Finally, the Data Protection Ombudsman pays attention to the fact that ICO's reply to the controller in 2018 did not concern the way in which the controller has collected consent to the processing of data belonging to special categories of personal data. In its reply, ICO stated that the controller has been able to request consent from the old users of [REDACTED], even though these users have already approved the processing of personal data when concluding a contract with the controller.

Data transfers to third countries

¹⁷ Guidelines for consent under Regulation 2016/679, point 61, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fi.pdf

¹⁸ Guidelines for consent under Regulation 2016/679, point 64, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fi.pdf



-
149. As a preliminary point, it should be noted that the controller's processing activities concerning transfer of personal data to third countries was based on the controller' procedure before 19 November 2019.
150. According to the controller, it is possible that the user's e-mail address or user ID will be transferred to a server located in the United States. The controller has reported that it has transferred data under the Privacy Shield. The Privacy Shield was repealed in the Schrems II decision of the Court of Justice of the European Union in July 2020. Thus, in February 2019 and at the time of the response given by the controller in November 2019, the controller has been able to transfer personal data to the United States on the basis of the Privacy Shield. The Data Protection Ombudsman's Office has not been informed of any transfer of data to non-EU/EEA countries other than the United States. Therefore, the transfer of data in this decision is limited to the question of the transfer of data to the United States.
151. The controller has based the transfer of data on data subjects' consent, in addition to the Privacy Shield. During the period at issue in the present case an adequate level of data protection has been guaranteed under the Privacy Shield. Therefore, there has been no need to use other legal basis as referred in Article 49 of the GDPR, for example consent.
152. As such, the GDPR does not require that in situations where personal data are transferred on the basis of explicit consent, the transfer should be occasional and non-repetitive". However, in its guidance on derogations under Article 49, the EDPB has highlighted that even those derogations which are not expressly limited to "occasional" or "not repetitive" transfers have to be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place.¹⁹ It should be noted that, in the present case, the transfer of data by the controller to third countries was not occasional and therefore the Article 49 derogation could not have been used in the present case as a basis for the transfer.
153. In the present case, as the transfer of data by the controller was based on the Privacy Shield, the controller had an appropriate basis for transferring data to the United States. In this context, it is not necessary to assess whether the consent collected by the controller has met the conditions laid down for consent. The current data transfer practices of the controller are also not assessed in the context of the present case.
154. The Data Protection Ombudsman states that the controller must not request consent to a particular processing of personal data simply to ensure that data subjects are more aware of the processing of their personal data after having given their consent. If the processing of personal data in certain situations does not require the explicit consent of the data subject, the consent should not be collected for the sole purpose of raising awareness. However, the Data Protection Ombudsman considers that the purpose of the controller

¹⁹ Guidelines 2/2018 on derogations of Article 49 under Regulation (EU) 2016/679 of 25.5.2018, page. 4-5 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fi.pdf



was good, as the controller has tried to raise the awareness of the data subjects.

Consent to the user content

155. According to the Terms of Use of [REDACTED], "by saving, submitting, or transferring content to [REDACTED] services, you are granting [REDACTED] an uncompensated, global, transferable, sub-licensable right to use, reproduce, present in public, edit, translate, and share your User Content".
156. The requirement of the [REDACTED] service is that a data subject accepts the Terms of Use. If a data subject does not wish to accept the above-mentioned processing operation described in the Terms of Use, a data subject does not get access to the [REDACTED] service.
157. First of all, it should be noted that the "accept" button should not be automatically interpreted as an act giving consent in accordance with the GDPR. In its clarifications, the controller has generally stated that the use of the [REDACTED] service requires consent. In the clarifications provided by the controller, the controller has not referred to any other legal basis other than consent, with the exception of processing of personal data for research and product development, in respect of which the controller has referred to a legitimate interest.²⁰ The Data Protection Ombudsman draws attention to the fact that, in written request for hearing of views and request for further clarification sent to the controller on 30 November 2021, the referendary of the Office of the Data Protection Ombudsman was of the opinion that consent to the processing of "user content" does not meet the conditions for consent provided for in the GDPR.²¹ In its reply to the written request for hearing of views and request for further clarification on 14 January 2022, the controller has not corrected referendary's assessment by noting that it has not been controller's intention to request consent to the processing of personal data for the processing of "user content". In other words, the controller has not stated in its reply that it has not processed personal data saved, submitted or transferred by the data subject on the basis of consent.
158. In the light of the clarifications provided by the controller, the Data Protection Ombudsman considered that by ticking the "accept" button on the Terms of Use, the controller intended to request consent to the processing of personal data regarding "user content" mentioned in the Terms of Use.
159. In this decision, the Data Protection Ombudsman does not assess whether consent has been an appropriate legal basis for the processing of personal data in connection with "user content". As presented below, the Data Protection Ombudsman's assessment is limited to whether the consent chosen by the controller as the basis for processing of personal data has been in accordance with Article 7(2) and (4) of the GDPR.
160. In its clarification, the controller specified "content" as follows: "Content" is not data from the user's device or data provided by the user when creating an account, but 'content' created by the user refers to information that the

²⁰ See paragraph 70 of the decision

²¹ Written request for hearing of views and request for further clarification, page 16



user chooses to share for example in discussions by groups provided by the controller or on the controller's social media channels. If the data subject decides to publish content by sharing, for example, a photograph on the social media channel of the controller, the data subject agrees, according to the Terms of Use, that the controller can, among other, copy, present publicly, edit and distribute content created by the user.

161. According to the controller, the [REDACTED] service has included functions that rely on content created by the user. Users have been able to share their results with followers managed by them, for example in the [REDACTED]-view and in the groups, events and clubs under the [REDACTED]-function. It has been possible to discuss the results in the abovementioned functions and views. Users have also been able to share training information with other users in the same group or event.
162. The Data Protection Ombudsman draws attention to the fact that the wording of the controller's information "*by saving, submitting, or transferring content to [REDACTED] services*" may have formed the impression to the complainant and possibly also for other data subjects that "content" refers to the information stored on the [REDACTED] service, for example during a sports performance. However, according to the controller, this is not the case. The controller does not use, copy, share publicly the user's training data in the [REDACTED] service. Instead, according to the Terms of Use, the controller could process the data in the manner described in the Terms of Use when the user distributes information on the controller's platforms, such as discussion forums. The above-mentioned assumption may also have been formed since the right of the controller to process content shared by the user has been specifically described in the [REDACTED]'s Terms of Use and not, for example, in the Terms of Use of the platforms offered and maintained by the controller ([REDACTED] and [REDACTED]).
163. According to the controller, the [REDACTED] service has included functions that rely on content created by the user. However, the Data Protection Ombudsman considers that the possibility to share images or discuss in the platforms is not the core service of [REDACTED], even though [REDACTED]-function and Syöte -view have relied on information obtained from the [REDACTED] service. The Data Protection Ombudsman is of the opinion that the core of the [REDACTED] service is monitoring the user's practice and analysing progress²². This view is supported by the fact that the sharing of information has been based on a voluntary approach by the user, as the user can use the [REDACTED] service without ever sharing the information or discussing on the data controller's platforms.
164. However, as explained above, the controller has included the processing of content created by the user in the general Terms of Use, to which the data subject was required to give their consent. Therefore, the data subject has been obliged to consent to processing in which the controller has a

²² According to the [REDACTED] website '[\[REDACTED\] is an exercise application and a training logbook online. When information about your traineeship, activity and sleep is available online, you can easily monitor your traineeship, analyse your progress and improve your results.](#)'



right to use, copy, present publicly, edit, translate and redistribute content shared by the user and obtained from the [REDACTED] service.

165. Consent is one of the legal basis for processing of personal data laid down in Article 6(1) of the GDPR. The consent to the processing of personal data must be, inter alia, specific and freely given. Specific consent of the data subject must be given in relation to “one or more specific” purposes. The controller must therefore make a clear separation of information related to obtaining consent for data processing activities from information about other matters.²³ According to Article 7(2) of the GDPR, if the data subject’s consent is given in the context of the written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The Data Protection Ombudsman is of the opinion that the controller should not have included in its general Terms of Use the activities concerning the processing of personal data for which it intends to seek consent under the GDPR.
166. As the consent collected by the controller to the processing of content created by the user has not been requested clearly separate from other matters, the consent has not been specified and therefore does not fulfil the requirement for consent under Article 7(2) of the GDPR.
167. In this context it should be noted that the Terms Use of the service should describe the general conditions of use of the service and the processing operations necessary of that service. For this reason, the Terms of Use should not include processing operations for which consent under the GDPR should be requested.
168. The element “free” implies real choice and control for data subjects. When assessing whether the consent has been freely given, account shall be given whether consent has been attached as part of terms that cannot be negotiated. If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given.²⁴ Account should also give to the Article 7(4) of the GDPR which states that when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. Compulsion to agree with the use of personal data additional to what is strictly necessary limits data subject’s choices and stands in the way of free consent. As data protection law is aiming at the protection of fundamental rights, an individual’s control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory

²³ Guidelines for consent under Regulation 2016/679, WP256, page 13-14 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

²⁴ Guidelines for consent under Regulation 2016/679, WP256, page 8 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf



consideration in exchange for the performance of a contract or the provision of a service.²⁵

169. The controller is of the opinion that the data subject has had the right to freely choose whether or not to share images or videos in the controller's service. The Data Protection Ombudsman notes that the data subject may in fact be able to choose themselves whether or not to share information about their exercises with other users. Nevertheless, the data subject has not had a genuine free choice to consent to the processing operations described in the Terms of Use for the processing of personal data and thus this consent did not meet the condition of a freely given.
170. The Data Protection Ombudsman also draws attention to the fact that the controller has stated in its Terms of Use that it is processing personal data on a very large scale. According to the Terms of Use of the controller, the user would give the controller "an uncompensated, global, transferable, sub-licensable right to use, reproduce, present in public, edit, translate, and share" content created by the user". The requirement for specific and freely given consent is also closely linked to the requirement of granularity. The consent should be granular and specific, i.e., the controller cannot request the consent of the data subject for undefined purposes or for unclear purposes. The Data Protection Ombudsman considers that the above description of the purpose of the processing is not sufficiently precise to enable the data subject to give freely given consent for specific processing activities of the controller.
171. Based on the above, the Data Protection Ombudsman considers that the consent collected by the controller to the processing of content created by the user laid down in Terms of Use has not, as a whole, met the requirements for consent referred to in Article 4(11) of the GDPR as the consent has not been, among other things, specific or freely given. As explained above, the consent has not been requested separately from other matters and it has not been possible to give consent free of choice, which is why the consent requested in this case did not meet the conditions for consent under Article 7(2) and (4) of the GDPR.
172. Data Protection Ombudsman draws attention to the fact that, as a matter of principle, content created by users may contain data concerning health. This must be taken into account when assessing the appropriate legal basis for the processing of personal data in connection with "user content", especially taken into account data subject's fundamental rights and freedoms.
173. Finally, the Data Protection Ombudsman states that, in the present decision, the Data Protection Ombudsman does not assess and it does not have competence to assess, from the point of view of the Copyright Act (404/1961), whether the data controller can process saved, submitted or transferred data without compensation and globally as described in the Terms of Use. In its decision, the Data Protection Ombudsman does not assess or otherwise take a position on the lawfulness of the processing. Thus, as regards the processing of 'user content', the Data Protection Ombudsman has limited its

²⁵ Guidelines for consent under Regulation 2016/679, WP256, page 11 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf



assessment to whether the consent requested by the controller to the concept of 'user content' fulfilled the conditions for consent in a situation where the processing of 'user content' was based on the data subject's consent.

The decision was made by the Data Protection Ombudsman [REDACTED], and it was presented by Senior Officer (referendary) [REDACTED].

According to section 24 of the Data Protection Act, the administrative fine is imposed by the Collegial Body for Sanctions, which has issued the following decision.



The decision of the Collegial Body for Sanctions

The controller

[REDACTED]

Decision

174. As is apparent from the decision of the Data Protection Ombudsman, the controller did not have specific and informed consent in accordance with the Article 4(11) and 9(2)(a) of the GDPR in order to process the maximum oxygen uptake and body weight index.
175. The case does not concern minor infringements of the provisions of the GDPR, as referred to in recital 148 of the GDPR, taking into account in particular the gravity of the breach, which is why a reprimand is not a sufficient sanction.
176. The Collegial Body for Sanctions states that there are a number of circumstances in favour of not imposing an administrative fine. When assessing the requirements for imposing an administrative fine, the Collegial Body for Sanctions has, however, paid particular attention to the fact that the large-scale processing of the special categories of personal data in question is an essential part of the controller's core business, which means that an administrative fine cannot be waived. However, these other factors are of considerable importance in assessing the amount of the administrative fine.
177. In this decision, the controller has infringed a provision under Article 83(5)(a) of the GDPR (Article 9). The infringement has thus concerned a violation of a higher category of administrative fine.
178. The controller's turnover for 2021 was [REDACTED]. In the present case, the administrative fine imposed to the controller shall not exceed EUR 20 000 000.
179. The Collegial Body for Sanctions jointly formed by the Data Protection Ombudsman and the Deputy Data Protection Ombudsmen orders the controller to pay an administrative fine of EUR 122 000 (one hundred twenty-two thousand) to the State under Article 58(2)(i) and Article 83 of the GDPR. The Collegial Body for Sanctions considers the administrative fine of EUR 122 000 to be effective, proportionate and dissuasive.

Grounds for imposing an administrative fine

The applicable legislation

180. Pursuant to Article 83(1) of the GDPR each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.



181. Pursuant to Article 83(2) of the GDPR administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). In the present case, the Data Protection Ombudsman has ordered the controller to bring its processing operations into line with the GDPR and issued a reprimand to the controller. The administrative fine is therefore imposed in addition to Article 58(2)(b) and (d).

182. 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.

183. Pursuant to Article 83(5)(a) of the GDPR, the infringements of the provisions in this paragraph (Articles 5,6,7,9) 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.

184. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, Article 83(1)(2) and (5) shall be taken into account. When assessing the matter, consideration shall also be given to the guidelines on the application and setting of administrative fines.²⁶

Assessment of the gravity of the infringement

²⁶ Guidelines on the application and setting of administrative fines (wp253) <https://ec.europa.eu/newsroom/article29/items/611237>



185. When assessing the gravity of the infringement, Article 83(2)(a)(b) and (g) of the GDPR have been taken into account.

Nature, seriousness and duration, nature, extent or purpose of the processing

186. Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. The legislator has therefore laid down specific requirements for the processing of personal data, such as the prohibition of their processing in principle and permitted only in the circumstances permitted by Article 9. The data at issue are data concerning health within the meaning of Article 9(1) of the GDPR. Although data concerns specific categories of personal data, the Collegial Body for Sanctions considers that this data is not particularly sensitive data (cf. data concerning mental health or, for example, data on insolvency or location, which are not to be considered as a specific categories of personal data).

187. The Collegial Body for Sanctions considers that even though the processing of special categories of personal data without sufficient conditions in accordance with Article 9 does not always itself lead to the imposition of an administrative fine, but when assessing the nature and purpose of the data processing in this case, special attention must be paid to the fact that the [REDACTED] service, and the data concerning health that is been processed in the service, are an integral part of the core activities of the controller. These factors, taken together, reflect the gravity of the infringement and advocate the imposition of an administrative fine.

188. As a mitigating factor, the Collegial Body for Sanctions considers that the purpose of the controller is not only to develop its own product, but the purpose has also been a specifically to provide to the data subject a service to improve the well-being of the data subject. Although the controller has benefited from the processing of maximum oxygen uptake and body weight index, the processing of these data has also benefited the data subjects, as the controller has been able to develop its service using the data it has processed. Nor was the earning logic of the controller's business based solely on the processing of the data subject's data.

189. Between 22 May 2018 and 18 February 2019, complaints were lodged with the Office of the Data Protection Ombudsman. The Data Protection Ombudsman has assessed the controller's practices in the above-mentioned period. The controller has continued to violate the GDPR also after the above-mentioned date, as the controller still does not request consent as referred in the GDPR for the processing of data on maximum oxygen uptake and body weight index²⁷. Based on the above, the controller's procedure under the GDPR be considered relatively long-term. However, the Collegial Body for Sanctions draws attention to the fact that the proceedings in the Office of the Data Protection Ombudsman have taken a long time. For this reason, the relatively long duration of the infringement cannot be considered to reflect the

²⁷ [REDACTED]'s website, visited on 9 September 2022



seriousness of the infringement, and this is not taken into account in the penalty assessment as a reason in favour of the administrative fine.

Number of the data subjects affected, and the level of damage suffered by them

190. As explained above, the activities of the controller have been examined with regard to complaints lodged in the Office of the Data Protection Ombudsman between 22 May 2018 and 18 February 2019. During this period, 3.47 million data subjects have approved the Terms of Use when registering for the [REDACTED] service. The controller has thus processed, or at least has been able to process, data on the maximum oxygen uptake and body weight index of 3.47 million users without a legal basis for the processing.
191. When assessing the impact of violations, account is taken not only of the number of data subjects but also of the fact that the processing of personal data was not just national, but the processing of personal data has also affected other data subjects located in the EU/EEA region.
192. On the one hand, the large number of data subjects reflects the seriousness of the infringement, but on the other hand according to the information available to the Office of the Data Protection Ombudsman, the data subjects have not suffered any financial damage.

The intentional or negligent character of the infringement

193. According to the guidelines issued by the Working Party, 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 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.²⁸
194. In addition to heart rate data, the controller has also requested consent to the processing of other special categories of personal data. As indicated in the decision of the Data Protection Ombudsman, the consent requested for the processing of other data concerning health did not meet the requirements of consent laid down in the GDPR. In this respect, the Collegial Body for Sanctions draws attention to the fact that the controller’s intention was to seek consent. Considering the whole, the Collegial Body for Sanctions considers that the infringement of the provisions of the GDPR cannot be considered intentional.
195. In its reply to the controller, the ICO stated that the controller has been able to change the grounds for processing, as a result of which the controller has been able to request the consent of old users²⁹. Although ICO has stated

²⁸ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, page 11 <https://ec.europa.eu/newsroom/article29/items/611237>

²⁹ see paragraph 30 of the decision: *In light of the information you have provided, we are satisfied that [REDACTED]’s actions relating to the change in lawful basis for processing to rely on consent, is in compliance with your data protection obligations.*



in its communication to the controller that the controller's actions complied with the obligations arising from data protection regulation, ICO has not specifically assessed the procedure for requesting consent, which is the subject of the present decision.

196. Furthermore, the Collegial Body for Sanctions is of the view that the clarifications provided by the controller in the matter show the controller's intention to comply with the obligations of the GDPR. This is reflected, among other things, by the fact that the controller has requested consent to the processing of other health data considered as sensitive data, even if the consent has not met the requirements for consent. The Collegial Body for Sanctions also states that the complaints relate to the time when the GDPR has just started to be applied.
197. Under the one-stop-shop mechanism, the Finnish Supervisory Authority, i.e., the Data Protection Ombudsman is responsible for the supervision of the processing of personal data by the controller in question. Although another supervisory authority has assessed controller's processing of personal data, the Collegial Body for Sanctions states that controllers should also be able to rely on the assessment carried out by the supervisory authorities of other Member States.
198. However, this is not an administrative decision of an authority, but an exchange of messages between the controller and ICO. Since the correspondence does not specifically concern the issue which the Data Protection Ombudsman has assessed in this decision, and since the data processing at issue concerns the controller's core activities, the Collegial Body for Sanctions considers that the controller cannot rely solely on the communication with ICO.
199. Consequently, the Collegial Body for Sanctions considers that the circumstances described in paragraphs 195 to 198 above cannot lead to the non-imposition of an administrative fine. However, facts presented in paragraphs 194 to 197 shall be taken into account as factors that significantly reduce the amount of the administrative fine.

The categories of personal data affected by the infringement

200. As stated in the Data Protection Ombudsman's decision, the controller's conduct that violates the provisions of the GDPR has concerned the processing of maximum oxygen uptake and body weight index, i.e data concerning the data subject's health, without consent as laid down in the under GDPR.
201. The Collegial Body for Sanctions has already assessed the significance of the nature in paragraphs 176 to 177 of the decision.

The assessment of the aggravating or mitigating factors

202. When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, Article 83(2)(c) – (f), (h) – (i) and (k) of the GDPR has taken into account.



Any action taken by the controller to mitigate the damage suffered by the data subject

203. According to the guidelines issued by the Working Party when a breach occurs and the data subject has suffered damage, the responsible party (controller) should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. In accordance with the guideline, the supervisory authority may when calculating the administrative fine, take into account such responsible operations of the controller or the absence of responsible operations.³⁰
204. The controller has not changed the consent collected to process maximum oxygen uptake and body weight index³¹. The Collegial Body for Sanctions does not consider this as an aggravating factor in the assessment of the fine, nor is it to be considered as a mitigating factor.

The degree of responsibility of the controller taking into account technical and organisational measures implemented by them pursuant to Article 25

205. Pursuant to Article 25 of the GDPR the GDPR requires that the controller shall take 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.”
206. As indicated in the decision of the Data Protection Ombudsman, the controller is of the opinion that the data processed by the controller cannot be used to draw conclusions on the current or future state of health of the data subject. Therefore, the controller has taken the view that it does not process data concerning health other than heart rate data. However, the controller has stated in its clarification that it processes maximum oxygen uptake and body weight index. In addition, the controller has stated on its website that the maximum oxygen absorption uptake it handles makes it possible to draw conclusions on the ability of the circulating system to transmit oxygen to the body.³²
207. On the basis of the above, the Collegial Body for Sanctions is of the opinion that the controller has not been properly ascertained as to whether it is processing other personal data concerning health and, and if so, which health data it is processing.

Any relevant previous infringements by the controller

³⁰ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, 3 October 2017, page 13 <https://ec.europa.eu/newsroom/article29/items/611237>

³¹ [REDACTED]’s website on 9 October 2022 [REDACTED].

³² see para 134 of the decision



208. According to the guidelines issued by the Working Party the supervisory authority should assess the track record of the entity committing the infringement. Supervisory authorities should consider that the scope of the assessment here can be quite wide because any type of breach of the Regulation, though different in nature to the one being investigated now by the supervisory authority might be “relevant” for the assessment, as it could be indicative of a general level of insufficient knowledge or disregard for the data protection rules.³³

209. Similar violations of the provisions of the GDPR have not been brought to the attention of the Data Protection Ombudsman. In addition, no measures referred to in Article 58(2) of the GDPR have been imposed on the controller on the same subject matter. The Collegial Body for Sanctions does not consider this as an aggravating factor nor it is to be considered as a mitigating factor.

The degree of cooperation with the supervisory authority, and the manner in which the infringement became known to the supervisory authority

210. According to the guidelines issued by the Working Party the degree of cooperation may be given “due regard” when deciding whether to impose an administrative fine and in deciding on the amount of the fine. Based on the guidelines, a note can be taken to the fact whether the entity responded in a particular manner to the supervisory authority’s requests during the investigation phase in that specific case which has significantly limited the impact on individuals’ rights as a result.³⁴

211. Pursuant to Article 31 of the GDPR the controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks. According to the guidelines issued by the Working Party, it would not be appropriate to give additional regard to cooperation that is already required by law.

212. The actions of the controller that violate the provisions of the GDPR have come to the attention of the Office of the Data Protection Ombudsman through complaints. The controller has cooperated with the Office of the Data Protection Ombudsman. In the assessment of the administrative fine, the Collegial Body for Sanctions does not consider the above-mentioned as an aggravating factor nor it is to be considered as mitigating factor.

Any other aggravating or mitigating factor applicable to the circumstances of the case

213. The Collegial Body for Sanctions shall take into account the loss of the controller’s business in recent years as a mitigating factor in the amount of the administrative fine.

³³ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, page 14 <https://ec.europa.eu/newsroom/article29/items/611237>

³⁴ Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, page 14 <https://ec.europa.eu/newsroom/article29/items/611237>



The decision to impose an administrative fine has been taken by the members of the Collegial Body for Sanctions.

Data Protection Ombudsman [REDACTED]

[REDACTED]

Deputy Data Protection Ombudsman [REDACTED]

[REDACTED]

Deputy Data Protection Ombudsman [REDACTED]

[REDACTED]

Senior Officer [REDACTED]

[REDACTED]

The document has been signed electronically. If necessary, the electronic signature can be verified by contacting the registry of the Office of the Data Protection Ombudsman.

Further information on this decision is provided by the referendary

Senior officer [REDACTED], tel. [REDACTED].

Applicable legal provisions

The General Data Protection Regulation ((EU) 2016/679) Articles 4(1)(11)(15)(22)(23)(24), 5(1)(a), 6(1)(a), 7(2)(4), 9(1)(2a), 13(1)(c), 49, 58(2)(b)(d)(i), 60(1,-6), 83(1)(2)(5).

Data Protection Act (1050/2018) 24 §

Administrative Procedure Act (434/2003) 25 §, 34 §

Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court by lodging an appeal in accordance with the provisions of the Administrative Judicial Procedure Act (808/2019). Appeals shall be lodged in the Administrative Court.

The appeal instructions are enclosed.

Service of notice



The service of notice of the decision shall be effected by post against a certificate of service in accordance with section 60 of the Administrative Procedure Act (434/2003).

Enclosures

Appeal instructions

Payment instructions of the administrative fine

Distribution

Controller

Applicants

Office of the Data Protection Ombudsman – contact information

Postal address: P.O. Box 800, 00531 Helsinki, Finland

Tel. (switchboard): +358 29 566 6700

E-mail: tietosuoja@om.fi

Website: www.tietosuoja.fi

Summary Final Decision Art 60

Complaints

Violation identified, Administrative fine.

EDPBI:LSA:OSS:D:2022:627

Background information

Date of complaint:	22 May 2018
Draft decision:	18 October 2022
Revised draft decision:	08 December 2022
Date of final decision:	27 December 2022
Date of broadcast:	27 December 2022
Controller:	[REDACTED]
Processor:	N/A
LSA:	FI
CSAs:	AT, IT, BE, CZ, FR, DK, EL, DE, HU, NL, NO, SK, SL, SE, LU, ES, PL
Legal Reference(s):	Article 4 (Definitions), Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), Article 7 (Conditions for consent), Article 9 (Processing of special categories of personal data), Article 13 (Information to be provided where personal data are collected from the data subject), Article 45 (Transfers with an adequacy decision), Article 46 (Transfers by way of appropriate safeguards), Article 49 (Derogations for specific situations)
Decision:	Violation identified, Administrative fine.
Key words:	Health records, Data subject rights, Lawfulness of processing, Consent, Administrative fine.

Summary of the Decision

Origin of the case

Between 22 May 2018 and 18 February 2019, five complaints concerning the controller were lodged with the LSA. A complaint lodged with the Austrian SA was transferred to the LSA so to handle the case jointly with the other five complaints. According to the complainants, the use of a heart rate monitor manufactured by the controller required the use of the controller's service and acceptance of the controller's Terms of Use and Privacy policy to which the complainants did not wish to consent. In order to use the service, the complainants had to give their consent to the following processing

operations: processing of personal data concerning the heart rate; transferring personal data outside the EU/EEA. The controller's Terms of Use stated the following, among other things: "By saving, submitting, or transferring content to the controller's services, you are granting an uncompensated, global, transferable, sub-licensable right to use, reproduce, present in public, edit, translate, and share your User Content. Excluding the rights related to your personal data, the rights you have granted to the controller are irrevocable." The controller's service was also offered in other EU/EEA Member States and the processing of personal data was subject to similar conditions, irrespective of the country in which the user was located. In addition to complaints, the LSA had, on its own initiative, initiated to investigate the processing of research and product development described by the controller in its Privacy Notice. According to the response given by the controller, the controller processed the personal data of users on the basis of a legitimate interest for research and product development purposes. The controller had also emphasised that the data was anonymous.

Findings

The LSA found that the controller had been obliged to request explicit consent to the processing of heart rate data on the basis of Article 9(2)(a) of the GDPR. The controller had not been obliged to inform about the processing of personal data in accordance with Article 13 of the GDPR when purchasing a heart rate device. In addition to the heart rate data, the controller also processed other data concerning the health of the data subject, when the controller was processing maximum oxygen uptake and the body mass index. The consent requested by the controller to the processing of other data concerning health had not been in compliance with the GDPR, and therefore the controller had not had a legal basis for processing other health-related data in accordance with Article 9(2) of the GDPR. At the time when the complaints were lodged, the controller had grounds to transfer data to the United States. The consent collected by the controller to the processing of user content did not comply with Article 4(11) of the GDPR and it did not meet the conditions for consent laid down in Article 7(2) and (4) of the GDPR.

Decision

The LSA ordered the controller to bring the consent collected for the processing of maximum oxygen uptake and the body mass index into compliance with the GDPR within three months for new data subjects, and within six months for existing data subjects from the date of receipt of the decision. The LSA ordered to assess whether, in addition to heart rate data, maximum oxygen uptake and the body mass index, the controller processed other health data belonging to special categories of personal data when combining user-related data in the controller's service. Where the controller processed data belonging to special categories of personal data, the controller had to ensure that it had consent under the GDPR to the processing of all data relating to health that it processed. The LSA also ordered to ensure, without delay of the date of receipt of the decision, that the controller had a legal basis pursuant to Article 6(1) of the GDPR to process personal data in connection with "user content". The LSA issued a reprimand to the controller under Article 58(2)(b) of the GDPR, as the consent requested by the controller to process the maximum oxygen uptake and the body mass index had not been in line with the GDPR. The controller had not had a legal basis for the processing of personal data that are an integral part of the controller's core business activity, which included the processing of data concerning health.

The LSA also imposed an administrative fine according to Article 83 of the GDPR. The controller infringed a provision under Article 83(5)(a) of the GDPR (Article 9). The infringement has thus concerned a violation of a higher category of administrative fine. The controller's turnover for 2021 was [REDACTED]. The LSA ordered the controller to pay an administrative fine of EUR 122 000 to the State under Article 58(2)(i) and Article 83 of the GDPR. The LSA considered the administrative fine of EUR 122 000 to be effective, proportionate and dissuasive.

Summary Final Decision Art 60

Complaint

Violation identified, Administrative fine.

EDPBI:FI:OSS:D:2022:604

Background information

Date of complaint:	26 October 2020
Draft decision:	10 November 2022
Revised draft decision:	N/A
Date of final decision:	09 December 2022
Date of broadcast:	15 December 2022
Controller:	[REDACTED]
Processor:	N/A
LSA:	FI
CSAs:	EE, NO, SE
Legal Reference(s):	Article 5 (Principles relating to processing of personal data), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 15 (Right to access by the data subject). Article 25 (Data protection by design and by default)
Decision:	Violation identified, Administrative fine.
Key words:	Health records, Accuracy, Right of access, Data subject rights, Transparency, Data protection by design and by default, Administrative fine.

Summary of the Decision

Origin of the case

On 26 October 2020, the complainant lodged a complaint with the LSA. The complainant alleged that the controller had maintained an extensive data file containing health information on its employees, this data file included the times of absence due to illness and the employees' diagnoses. The data of the complainant was stored in this file for 20 years and the data in the file was also partly inaccurate. Furthermore, the complainant alleged that this data was used against her when she contested her dismissal. She has asked the controller for access to her personal data and said that she has requested

access to the log data related to the data file in question. The complainant has not been given access to the log data. Information on the diagnose listing included in the data file had not been given to the complainant. The information provided by the controller confirmed that it had maintained two data files intended for internal use (the MAPS human resources management system and Medakt patient record system), which had contained employees' health information, among other things. The controller had processed employees' health information for the payment of sick pay or comparable benefits linked to the employee's health. When an employee had fallen ill while working on a ship, the ship's nurse had recorded this in the Medakt patient record system. If the illness led to sick leave, this was recorded in the MAPS system after the employee had delivered the sick leave certificate. Health information had only been processed by the employees of the controller tasked with preparing, making or implementing employment-related decisions based on such information. At the moment of the decision of the LSA, the data in the Medakt system had been stored for an indefinite period. Data subjects had the right to review data saved in the MAPS and Medakt systems. The data had also been updated, when necessary. According to the information provided by the controller, the information on the complainant's sick leave certificates was given to the complainant insofar as it was available. The oldest information had already been erased.

Findings

The LSA found that the controller: had not complied with the provisions of the Working Life Privacy Act when saving diagnoses into the MAPS system; had not complied with the provisions of the Working Life Privacy Act when storing its employees' health information in the MAPS system; had not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR in order to ensure that the personal data processed in the MAPS system was accurate and up to date; had not complied with the provisions of Article 5(1)(a) and Article 13 of the GDPR; had not complied with the provisions of Article 12(3) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR; had not complied with the provisions of Article 15(1) of the GDPR when replying to the complainant's request made pursuant to Article 15 of the GDPR. The LSA found that the employer nevertheless had the right to process, for example in its HR systems, data concerning the dates and lengths of an employee's absence from work due to sick leave. However, information on the causes of the absence due to illness, such as the disease or injury or its nature or diagnosis, may not be saved into HR systems. The medical certificates or statements delivered to the employer by the employee must be stored separately from other personal data concerning the employee. The LSA found that the controller had not presented any grounds by virtue of which the complainant's data could have been stored for 20 years in the MAPS system nor any justification for retaining the health information of its employees in the MAPS system for ten years from the end of the absence. The LSA found that the controller had not taken every reasonable step under Article 5(1)(d) and Article 25(1) of the GDPR to ensure the accuracy of the personal data processed in the MAPS system. The Deputy Data Protection Ombudsman thus finds that the controller had not complied with the provisions Article 5(1)(a) and Article 13 of the GDPR. Since information on the complainant's diagnoses was later disclosed to the police, the LSA found that the basis for the disclosure may be assessed as a criminal matter. The complainant may turn to the police on this matter.

Decision

The LSA issued a reprimand to the controller under Article 58(2)(b) of the GDPR. The controller had not complied with the following provisions referred to in Article 83(5) of the GDPR: 1) Article 5(1), points (d) and (a); 2) Article 13; 3) Article 12 (3); 4) Article 15(1) And 5) 25(1) of the GDPR. The LSA found an administrative fine of EUR 230,000 to be effective, proportionate and dissuasive.



24 June 2021

Record no. 4182/146/2019

Decision of the Data Protection Ombudsman

Matter Right of access to data

Complainant [REDACTED]

Data controller [REDACTED]

On 4 March 2019, the complainant has instituted a matter with the Danish Supervisory Authority (Datatilsynet) concerning a data subject's right of access to data. The complainant has stated that he has requested access to his data from the controller. The data controller has confirmed the receipt of the complainant's request on the same day, 12th November 2018. Later, on 12th December 2018, the data controller has communicated that they will provide the requested data within the 60 days referred to in Article 12, Paragraph 3 of the General Data Protection Regulation. This never happened. The Danish Supervisory Authority has contacted the controller at a later time, and the controller has informed the Danish supervisory authority on 27th March 2019 of its intent to provide the complainant with the requested data. In a telephone conversation on 20th May 2019, the complainant has, however, informed the Danish Supervisory Authority that he has not received the data in question.

The Danish Supervisory Authority has completed a preliminary assessment of the matter, investigating, inter alia, its cross-border nature. With regard to this, the controller has pointed out that the headquarters of the company, [REDACTED], [REDACTED], are located in France. However, according to the preliminary assessment, these French headquarters do not make decisions on processing personal data that is the subject matter of this complaint, nor do they have the competence to implement these decisions. Instead, the decisions are made and implemented by [REDACTED], a company operating in Finland, Sweden, Norway, and Denmark and in Estonia, Latvia and Lithuania, with headquarters in Finland. The preliminary statement submitted to the Danish Supervisory Authority furthermore indicates that personal data is processed in all of the aforementioned locations. The decisions concerning personal data processing which are the subject matter of the complaint are made and implemented in Finland, which means that the Finnish Supervisory Authority (The Office of the Data Protection Ombudsman) has been determined to be the competent lead supervisory authority in the matter.

Information provided by the controller

The Office of the Data Protection Ombudsman has requested that the controller provide more information on the matter. The controller has submitted a statement on 12th May 2020.

The statement provided confirms that the complainant has requested access to his information on 12th November 2018. The statement furthermore indicates that the controller has determined detailed procedures for ensuring that such requests by data subjects will be identified and processed in an appropriate manner, and on submitting the



requested information to the data subject within the set deadline. The controller has furthermore stated that its failure to submit the data to the complainant has not been intentional.

The submitted statement also explains that the requested information has been collected and processed for the purpose of being sent to the complainant. Regarding this, the controller has notified that they have divided the material into written documents and telephone call recordings. The controller has also stated that it has not submitted the telephone call recordings, because the third party on the telephone calls was recognizable. The controller has, however, stated that in the future, recordings will be made available to the data subjects in the future for listening.

With regard to the written materials, the controller has stated that they were not submitted to the complainant due to a human error. The controller has made it known that they will find out the reasons behind this error. Due to the Covid-19 pandemic, several employees of the controller were temporarily laid off at the time of the investigation, which has complicated the process. The controller has also stated that they have updated their procedures and guidelines regarding the use of right of access. The controller has stated that they are confident that they can minimize the occurrence of similar human errors in the future and that all requested information will be provided in due time.

Additional information provided by the controller

The Office of the Data Protection Ombudsman has requested that the controller provide additional information on the matter. The controller has submitted an additional statement on 20th August 2020.

The controller has stated that they have subsequently delivered the complainant the data he had requested, excluding the telephone call recordings. The complainant was not offered the telephone call recordings because the controller has wanted to ensure that there will be no violation of the rights and data protection of a third party that appears on the recordings and can be recognized. The controller has stated that they have taken measures to comply with the contents of the decision of the Deputy Data Protection Ombudsman, no. 3021/452/2017. The controller has suggested that in the future, it will be possible to produce transcripts of the recorded telephone calls to make the third party unrecognizable, and to submit these transcripts to the data subject requesting access to their data. For clarity's sake, the controller has noted that it is not in possession of telephone recordings concerning the complainant. The telephone recordings are deleted from the controller's systems six months after the telephone call.

The complainant's response

The complainant has submitted a response on 14th October 2020.

The complainant has confirmed that the controller has submitted him the data in question. The controller has also reserved the complainant an opportunity to visit their office to listen to the recordings of telephone conversations which were, at the time, in the possession of the controller.

The complainant is not satisfied with the controller's course of action. The complainant has mentioned that the procrastination by the controller has caused him to suffer losses



of right. The complainant had numerous problems with the vehicle he had purchased. The complainant claims that due to the procrastination of the controller, he has been forced to ultimately sell his vehicle. According to the complainant, he has lost approximately DKK 75,000 (\approx EUR 10,000, estimate by the complainant). The complainant has not been able to keep a vehicle that has to be repaired constantly. Due to the complainant being refused access to data, he has not been able to bring the matter to be assessed by a competent authority. The controller has refused to compensate the costs accrued to the complainant. The complainant does not think it is right or fair that he has had to wait for his data for over 18 months.

Applicable legislation

The General Data Protection Regulation of the European Parliament and of the Council ((EU) 2016/679, the GDPR) has been applied as of 25 May 2018. As a regulation, the GDPR is directly applicable in Member States. The GDPR is supplemented by the Finnish Data Protection Act (no. 1050/2018) that has been in force since 1 January 2019. The Data Protection Act repealed the Personal Data Act (523/1999).

Evaluation of cross-border factors

The General Data Protection Regulation separately sets forth provisions on cross-border processing of matters, as laid down in Article 4, Paragraph 23 of the GDPR. These matters must be processed by a competent supervisory manner in the manner laid down in Article 56, Chapter VII.

The controller's preliminary statement points out that the headquarters of the company [REDACTED] are in France. However, according to the preliminary assessment, these headquarters in France do not make decisions on processing personal data to which this complaint focuses, nor do they have the competence to implement these decisions. Instead, the decisions are made and implemented by [REDACTED], a company operating in Finland, Sweden, Norway, Denmark and Estonia, Latvia and Lithuania. The headquarters of this company are located in Finland. The preliminary statement submitted to the Danish Supervisory Authority furthermore indicates that personal data is processed in all of the aforementioned locations. Due to these factors, the Data Protection Ombudsman finds that, by virtue of Article 56 of the General Data Protection Regulation, the Data Protection Ombudsman is the competent lead supervisory authority in this case.

Judicial question

As stated above, the Data Protection Ombudsman shall review and decide on the case based on the General Data Protection Regulation (EU) 2016/679, and the Data Protection Act (1050/2018).

In the case of the complainant, it must be assessed if the controller has taken the measures required for the complainant to exercise their right of access to data in accordance with Article 12(1 and 3), and Article 15(3) of the General Data Protection Regulation. The Data Protection Ombudsman will additionally assess if it should apply the corrective powers bestowed on to it under Article 58(2) of the GDPR.

Decision of the Data Protection Ombudsman



The controller has not taken the measures for the complainant to exercise their right of access to data as laid down in Article 12(3) of the GDPR.

The controller has not provided the complainant with the telephone call recordings in accordance with Article 12(1) and Article 15(3) of the GDPR.

The Data Protection Ombudsman issues a reprimand to the controller by virtue of Article 58(2b) of the GDPR. The controller has not provided the complainant with access to data referred to Article 15 of the GDPR without undue delay or the deadline laid down in Article 12(3) of the GDPR. Regarding the telephone calls, the controller has not taken the measures for the complainant to exercise their right of access to data as laid down in Article 15 of the GDPR.

The Data Protection Ombudsman shall issue a reprimand to the controller in accordance with Article 58(2d) of the GDPR, ordering the controller to change their processing procedures so that the data subjects will be able to exercise their right of access to data in accordance with Article 12(1 and 3), and Article 15(3) of the General Data Protection Regulation.

Grounds

Article 15(1) of the GDPR sets forth 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 and the information referred to in the sub-paragraphs of Article 15(1). Similarly, in accordance with Article 15(3) of the GDPR, the controller shall provide a copy of the personal data undergoing processing.

By virtue of 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.

According to Article 12(1) of the GDPR, the controller shall take appropriate measures to provide any information relating to processing to the data subject referred to under Article 15 in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. In accordance with Article 12(2) of the GDPR, the controller shall facilitate the exercise of data subject rights under Articles 15 to 22.

Article 15(4) of the GDPR sets forth that the right to obtain a copy shall not adversely affect the rights and freedoms of others, and according to Paragraph 63 of the Recitals of the GDPR, these include trade secrets or intellectual property and in particular the copyright protecting the software, and based on this, it is as such possible to refuse to provide the data referred to in Article 15(1). According to Article 15(4) of the GDPR, it is possible in some cases to refuse to submit a copy of the data referred to in Article 15(1). However, the contents of the aforementioned provision do not constitute an



acceptable reason for refusing the data subject to exercise their right of access to all information.

The present case

The complainant has confirmed that the controller has submitted him the data in question, exclusive of the telephone call recordings. The data was not, however, provided without an undue delay nor was it submitted within the deadline laid down in Article 12(3) of the GDPR.

The complainant has requested access to his data initially on 12th November 2018, and on 12th December 2018, the data controller has informed the complainant that the requested data will be provided within the 60-day period referred to in Article 12(3) of the General Data Protection Regulation. This has, however, not happened, due to which the complainant has contacted the Danish Supervisory Authority that has later contacted the controller. The controller has informed the Danish Supervisory Authority on 27th March 2019 of its intent to provide the complainant with the requested data. In a telephone conversation on 20 May 2019, the complainant has, however, informed the Danish Supervisory Authority of not receiving the data in question.

The Office of the Data Protection Ombudsman has sent the controller a request for information on 16th May 2020. The controller has submitted a statement on 12th May 2020. The statement indicates that the information was not submitted to the complainant due to a human error. The Data Protection Ombudsman wants to point out that the controller has not, at this point, committed to rectifying the situation. The controller has not promised to take the measures required to ensure that the complainant could exercise his right of access. An additional request for information has been presented to the controller on 7th August 2020, and the controller has submitted an additional statement on 21th August 2020. The additional statement provided indicates that the information has been delivered to the complainant with the exception of the telephone call recordings. It must be noted here that the complainant has requested for his data initially in November 2018, and it was finally delivered to him in August 2020. Thus, it has taken one year and nine months for his right to be realized. It can be stated that, despite the requests of the complainant and the contacts taken by the data supervisory authority, the controller has not taken the measures to ensure that the complainant can exercise his right appropriately. The controller's acts have violated the provisions of Article 12(3) of the GDPR.

Telephone call recordings

The controller did not provide the complainant with the telephone call recordings due to the controller's need to avoid the violation of the rights and data protection of the third person on the recordings, who is recognizable on the tapes.

It must be noted for clarity's sake that the recording includes personal data referred to under Article 4(1) of the GDPR. In its decision no. 2094/1/09, granted on 30 July 2010, the Supreme Administrative Court of Finland has determined that a voice captured on a tape is a piece of personal data, and thus the right of access laid down in Section 26 of the Finnish Personal Data Act (523/1999, repealed on 01/01/2019) applies to it. Similarly, a Court of First Instance of the European Communities has on 11 March 2009 interpreted in the case T-166/05 that a person can be identified by their voice (Section



39). Thus, a person's voice must be deemed an item of personal data. The GDPR has not amended the definition of personal data as laid down in the Personal Data Act.

The GDPR's entry into force and its application have not changed the definition of personal data in such a manner that the interpretation of a voice captured on tape as personal data would need to be re-evaluated. Thus, the data subject will continue to have a right of access to personal data also with regard to the telephone call recordings. It must be stated that the Deputy Data Protection Ombudsman's decision, no. 3021/452/2017 (issued 20/02/2020) also follows the aforementioned legal practice and conforms to the interpretation.

Let it also be noted that Article 15(4) of the GDPR sets forth that the controller can refuse to submit a copy of the data if the exercise of this right could adversely affect the rights and freedoms of others. To be able to restrict the rights of data subjects based on the aforementioned provision the controller must, however, be able to indicate that exercising the right of the data subject will adversely affect the rights and freedoms of others as referred to under Section 15(3) of the GDPR. It must be stated that recording the voice of a person who is doing their job cannot be considered to constitute such a reason.

It must additionally be stated the Data Protection Ombudsman has interpreted, in their decision no. 2240/523/2013 issued on 12/09/2013 under the repealed Personal Data Act, that telephone call recordings contain in practically all cases personal data of another person, and this cannot be deemed a reason to refuse the right of access. According to this decision, personal data of the controller's representative could have been submitted to a data subject who is exercising their right of access without constituting a breach of the Personal Data Act.

The controller did not provide the complainant with the telephone call recordings, but they did reserve the complainant the right to listen to the recordings at the controller's office.

The Data Protection Ombudsman has furthermore made the interpretation in its decisions under the repealed Personal Data Act (issued on 10/05/2011, record no. 2680/41/2010 and issued on 12/09/2013, record no. 2240/523/2013) that a data subject is entitled to the customer call recordings by virtue of Section 28 of the Personal Data Act. The Data Protection Ombudsman has viewed that the measures taken to exercise the right referred to under Section 26 of the Personal Data Act can include reserving the data subject an opportunity of listening to the telephone call recording (2680/41/2010) or by providing a written copy of the recording to the data subject as per their request, for example as a print-out of a transcribed document (2240/523/2013). However the data must be submitted in written form as per the request of the data subject (12/09/2013, record no. 2240/523/2013). It must be stated that the Deputy Data Protection Ombudsman's decision, no. 3021/452/2017 (issued 20/2/2020) also follows the aforementioned legal practice and conforms to the interpretation.

The GDPR also includes provisions on the form of the data provided. According to Article 12(1) of the GDPR, the information that applies to Article 15 shall be provided in writing, or by other means, including, where appropriate, by electronic means. Furthermore, regarding the right of access to data, Article 15(3) of the GDPR sets forth that the controller shall provide a copy of the personal data undergoing processing.



The Data Protection Ombudsman finds that with regard to the telephone call recordings, offering the opportunity to listen to the recordings does not comply with the provisions of Article 12(1) and Article 15(3) of the GDPR. According to Article 12(1) of the GDPR, *the information shall be provided in writing, or by other means, including, where appropriate, by electronic means*. Similarly, in accordance with Article 15(3) of the GDPR, *the controller shall provide a copy of the personal data undergoing processing*. In this respect, the Data Protection Ombudsman wants to draw attention particularly to the fact that any restrictions to the right of access to data that is laid down in Article 8(2) of the Charter of Fundamental Rights of the European Union (2012/C 326/02) must be narrowly interpreted.

The Data Protection Ombudsman finds that the controller is entitled to offer the data subject the opportunity to listen to the telephone call recordings in the controller's office, if they so wish, but this cannot be the only measure taken to ensure that the data subject can exercise their right of access.

The repealed Personal Data Act would have placed the obligation to the controller to submit the data requested by the data subject in a written form, for example in a transcribed file. The GDPR allows the data to be submitted in electronic form, which means that the controller could, at their discretion, to submit a copy of the data in some other form, for example as a recording.

The additional information provided indicates that the controller is no longer in the possession of the telephone call recordings that concern the complainant. The additional information provided furthermore indicates that telephone recordings are deleted from the controller's systems six months after the telephone call. In this context, it must be stated that the Data Protection Ombudsman cannot issue an order for the data subject to have a right of access to data that is not in the controller's possession (cf., *inter alia* Decision by Helsinki Administrative Court 19/0154/5, issued on 07/03/2019).

Based on the aforementioned, the Data Protection Ombudsman concludes that the controller has not taken the required measures for the complainant to exercise their right of access to data as laid down under Article 15 of the GDPR, and the controller's course of action with regard to ensuring the data subject's right of access to the telephone call recordings, does not comply with the provisions of Article 12(1) and Article 15(3) of the GDPR in general.

Applicable legal provisions

As referred to under Grounds.

Appeal

According to Section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court by lodging an appeal in accordance with the provisions of the Administrative Judicial Procedure Act (808/2019). Appeals shall be lodged in the Helsinki Administrative Court.

The appeal instructions are enclosed.

Service of notice



The service of notice of the decision shall be effected by post against a certificate of service in accordance with section 60 of the Administrative Procedure Act (434/2003).

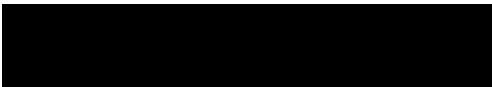
Further information on this decision is provided by the referendary

Senior Officer's name and telephone number

The Data Protection Ombudsman



Senior Officer



The document was signed electronically. The authenticity of the signature can be verified with the registry of the Office of the Data Protection Ombudsman.

Appendices

Appeal instructions

Distribution

Complainant

Controller

Contact information of the Office of the Data Protection Ombudsman

Postal address: P.O. Box 800, FI-00531 Helsinki, FINLAND

E-mail: tietosuoja@om.fi

Switchboard: +358 (0)29 566 6700

Website: www.tietosuoja.fi

Decision No. MED 2022-079 of 8 September 2022 issuing an order to the company,

[REDACTED]
(No. MDM221085)

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

Having regard to amended Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to the decision of the Chair of the French Data Protection Authority (CNIL) no.2021-183C dated 29 June 2021 of the Chair of the CNIL to instruct the Secretary-General to carry out or have carried out a verification of the compliance of the personal data processing carried out by or on behalf of [REDACTED];

Having regard to the online investigation record no. 2021-183/1 of 05 August 2021;

Having regard to the onsite investigation record no. 2021-183/2 of 28 September 2021;

Having regard to the other documents in the case file;

I. The procedure

Created in 2009, under the name [REDACTED] the company called [REDACTED] since 2012 (hereinafter "the company"), whose registered office is located at [REDACTED] operates an online sales platform that connects buyers and sellers of second-hand luxury clothing and fashion accessories.

The company employs [REDACTED] employees worldwide and achieved turnover of [REDACTED] in 2020, including [REDACTED] in France.

It has subsidiaries in Germany and Italy, which are mainly in charge of logistical aspects.

Approximately 13 million users are registered on the platform, of which approximately 9 million are located throughout all Member States of the European Union, and in particular 3,872,538 in France, 1,250,899 in Italy, 876,141 in Germany, 590,073 in Spain and 244,074 in Belgium.

The website and application are available in several languages (English, Italian, Spanish).

The processing operations are carried out in the same way, regardless of the user's country of residence.

Pursuant to Decision No. 2021-183C of 29 June 2021 of the Chair of the Commission nationale de l'informatique et des libertés (hereinafter "CNIL"), a CNIL delegation carried out an online investigation on 5 August 2021, then on 28 September 2021, an on-site investigation vis-à-vis the company located (as of the date of the inspections) at 255, boulevard Pereire in PARIS (75017), for the purpose of verifying the compliance of the personal data processing carried out by company or on its behalf, within the provisions of the aforementioned (EU) 2016/679 regulation (hereinafter "GDPR" or "Regulation") and amended Law No. 78-17 of 6 January 1978 and, where applicable, the provisions of Articles L. 251-1 et seq. of the Internal Security Code.

The delegation also focused on monitoring compliance with the provisions of Article L.34-5 of the French Postal and Electronic Communications Code (CPCE).

The platform offered by the company is accessible from the website [REDACTED] or from the [REDACTED] app, available on all Android and iOS app stores, for mobiles.

The company has two business models:

- either direct contact, with the direct sending of the product by the seller to the buyer. In this case, the company deducts a purchase commission;
- or contact with authentication of the product by [REDACTED]: the buyer sends the product to the company for verification, which then makes the delivery to the buyer. In this case, the company deducts a commission on purchase as well as an additional verification fee.

On 8 October, 24 November 2021 and 13 January 2022, the company sent the additional documents requested during the inspections and at the time of the verifications which followed concerning, in particular, the nature of the personal data collected and its retention period, the data processing agreements and the security and confidentiality of the personal data processed.

On 6th July 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

No relevant and reasoned objection has been expressed by one of the relevant authorities.

II. Breaches of the GDPR

1. *Breach of the obligation to define and comply with a personal data retention period in proportion to the purpose of the processing*

Article 5(1)e of the GDPR provides that "*personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [...] (storage limitation)*".

The CNIL recalls, by way of illustration, in its practical guide on retention periods (https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf), that in the absence of a text defining the retention period, "*it is the responsibility of the data controller, pursuant to the general principle of responsibility, to define said period. To do so, it must rely on the purpose for which the processing of personal data is implemented, i.e. the purpose it pursues. It is therefore necessary to identify and assess its operational needs. On the basis of these elements, a period to be applied, or, at least, the criteria for setting it (for example: the time of the business relationship) will thus be defined*" (practical guide, p. 7).

In this respect, by way of clarification, the reference guidelines relating to processing personal data implemented for the purposes of managing commercial activities recommend, in particular, that the data necessary for the performance of a contract or management of the commercial relationship be kept in an active database only for the duration of the contractual and commercial relationship. At the end of said period it must be deleted or anonymised. In some cases, after sorting the personal data processed, part of these data may be archived – in particular for compliance with legal obligations – or retained for other purposes, for example for marketing purposes.

With regard, specifically, to commercial activities that involve the creation of an online account by clients, the reference guidelines specify that the data are intended to be kept until the user deletes the account. However, it is common for users to no longer use these accounts without deleting them, which leads them to continue indefinitely and is contrary to the principle of limitation of data retention laid down by Article 5(1)e of the Regulation. In this case, the CNIL recommends that the accounts be considered inactive after two years and be deleted at the end of this period, unless the user expresses their wish to keep the account active.

In this case, no data retention policy has been defined by the company, with said company indicating that it retains user data for a period of 3 years from a user's last interaction with the platform.

However, the delegation was able to observe in the database:

- 5,646,633 accounts whose last connection was more than 3 years ago,
- 2,556,507 accounts whose last connection was more than 5 years ago,
- 716,481 accounts whose last connection was more than 8 years ago.

The retention of personal data of inactive users for more than 3 years therefore appears excessive.

Moreover, the company clarified that no automated data deletion process was implemented. However, in view of the volume of data processed, only automatic purge or archiving rules would be able to guarantee compliance with the retention periods.

Consequently, keeping user data for a longer period than that defined in its retention policy constitutes a breach of Article 5(1)e of the GDPR.

It is therefore the company's responsibility to effectively implement its personal data retention policy vis-à-vis the data that it processes.

2. Failure to provide a formal legal framework for the processing operations carried out on behalf of the data controller

Article 28(3) of the GDPR provides that any processing carried out by a data processor must be governed by an agreement concluded between the data controller and the data processor which "defines the purpose and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the obligations and rights of the data controller". This agreement must therefore provide for a set of mandatory information, detailed in points a) to f) of the same article.

In this case, the delegation found that certain agreements entered into with data processors did not contain all the information required by Article 28 of the Regulation. Namely:

- the agreement entered into with [REDACTED], which does not contain any information relating to the details of the processing operations carried out (notably, the agreement does not define the reason, nature and purpose of the processing);
- the agreement with [REDACTED] which does not contain a clause providing for the assistance of the data processor in carrying out an impact assessment, or an obligation for the data processor to inform the data controller in the event of instructions that would be contrary to the GDPR.

The company indicated to the delegation that it had sent draft amendments to the data processors concerned by the incomplete agreements. However, the company has not provided either the amendments sent or the list of data processors concerned. Nor did the company inform the CNIL of the progress of the negotiations for their signature.

These elements therefore constitute a breach of Article 28 of the Regulation.

3. A breach of the obligation to ensure the security and confidentiality of personal data

As data controller within the meaning of the GDPR, the company is subject to the obligations relating to the security of the personal data processing that it performs.

In this respect, Article 32.1 of the GDPR provides that: "*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*", and notably "*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*".

Firstly, the CNIL highlights that the National Information Systems Security Agency ("ANSSI") had the opportunity to recall the best practices to be applied in this area: "*Any person accessing a sensitive IS resource must be identified and authenticated by means of an individual account*" (Recommendations for the architecture of sensitive or confidential restricted

distribution information systems of 28 December 2020) Moreover, "*Identifiers and secrets associated with administrative accounts, whether technical or business, are part of the first computer attack targets because they have high privileges. It is therefore necessary to be very vigilant about the management of these identifiers and secrets, by adopting at least the following measures and choosing equipment that authorises their implementation: [...] use of individual administration accounts instead of generic accounts where possible*" (Recommendations on the security of physical access control and video protection systems of 4 March 2020).

The CNIL then highlights that only individual accounts allow for good traceability of accesses and actions carried out on the information system. The CNIL also notes that shared accounts do not allow proper application of the authorisation policy. However, the latter is a fundamental element of the security of information systems, aimed at limiting access to the data that a user needs (CNIL guide <https://www.cnil.fr/fr/securite-gerer-les-habilitations>). Indeed, the shared accounts make the accountability of an action much more difficult and complicate the investigation work in the event of a security incident.

Lastly, with regard to passwords, the CNIL highlights that, in accordance with the basic rules on information system security, in order to be effective a password must remain secret and individual. However, when an account is shared between several individuals, this rule is no longer respected.

In this case, the delegation noted that all members of the on-call team in charge of managing the database used a shared account, which does not allow for the proper logging of actions or tracing potential security incidents. Said configuration also jeopardizes the confidentiality of the password for the account concerned.

These facts constitute breaches of Article 32 of the GDPR, which imposes on the data controller the implementation of means to ensure the security of the personal data processed. The company must therefore set up named accounts for members of the on-call team in charge of managing the database.

III. A breach of Article L.34-5 of the French Postal and Electronic Communications Code (Not submitted to the cooperation procedure)

In application of Article L.34-5 paragraph 1 of the Postal and Electronic Communications Code (CPCE), "direct prospecting by means of an automatic calling, fax or email system using, in any form whatsoever, the contact information of a natural person who has not expressed his or her prior consent to receiving direct prospecting by that means, is prohibited".

Paragraph 4 of the same article specifies that direct e-mail marketing is authorised if the recipient's contact details "have been collected from him/her, in compliance with the provisions of French Data Protection Act No. 78-17 of 6 January 1978, in connection with a sale or provision of services, if the direct marketing concerns products or services similar to those previously provided by the same natural person or legal entity, and if the recipient is offered, expressly and unambiguously, the opportunity to object, without charges, other than those related to the transmission of the refusal, in a simple manner, to the use of his/her contact details at the time they are collected and every time a marketing e-mail is sent to him/her if he/she has not initially refused such use".

In this case, the delegation was informed that when a user sells or buys products on the [REDACTED] platform, said user is then likely to receive marketing emails on the basis of the exception of similar products and services provided for in Article L.34-5 of the CPCE.

Nevertheless, when registering, the user does not have the option of objecting to the receipt of these subsequent emails.

Therefore, if the company fails to offer said option, these facts constitute a breach of the obligations arising from Article L. 34-5 of the French Postal and Electronic Communications Code.

Consequently, [REDACTED], located at [REDACTED]
[REDACTED] is hereby ordered, within three (3) months of notification of this decision, and subject to any measures it may have already adopted, to:

- effectively implement its personal data retention period policy, which must not exceed the period necessary for the purposes for which the data are collected and proceed with purging or, where applicable, archiving the data stored at the end of the planned retention period, and in any event – concerning the data of users of the platform considered as inactive – by deleting the data of users who have been inactive for more than 3 years;
- ensure that the data processing agreements contain all the information provided for in Article 28 of the Regulation;
- take all security measures, for all personal data processing that it implements, to preserve the security of said data and to prevent unauthorised third parties from having access to the data, by setting up personal accounts for members of the on-call team concerning the management of the database;
- refrain from sending marketing emails based on the exception of similar products or services without having previously offered the recipients, expressly and unambiguously, the possibility of objecting, free of charge and simply, to the use of their contact details at the time said details are collected;
- provide supporting documentation to CNIL that all of the aforementioned claims have been complied with within the time limit set.

At the end of the period, if [REDACTED] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to the company to that effect.

Conversely, if [REDACTED] has not complied with this order by the end of the period, a rapporteur will be appointed who may request that the restricted committee to issue one of the sanctions provided for by Article 20 of the amended Act of 6 January 1978.

The Chair

Marie-Laure Denis

[REDACTED]
Chief Executive Officer
[REDACTED]

**REGISTERED LETTER WITH
ACKNOWLEDGEMENT OF RECEIPT**
[REDACTED]

Investigation of the case:

Paris, on **24 MAI 2023**

Our Ref.: [REDACTED] CM

Referral no. [REDACTED]
(to be quoted in all correspondence)

For the attention of the Chief Executive Officer,

I am following up on the exchanges that took place between the departments of the *Commission nationale de l'informatique et des libertés* ("CNIL" – French data protection authority) and the data protection officer of [REDACTED] (referred to as "VP Legal & Compliance") as part of the investigation of [REDACTED]'s complaint, forwarded by the Hamburg data protection authority, in application of the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complainant lodged a complaint with his national data protection authority on 27 June 2022 against [REDACTED], a company established in France, for failing to take sufficient measures to comply with his request to erase all his personal data.

In particular, the complainant indicated that he had requested the erasure of all personal data concerning him and the deletion of his user account on 20 June 2022. On the same day, your customer service would have confirmed the deletion of his account and the deletion of said data by specifying that he would no longer receive commercial prospecting emails. However, the complainant received a commercial prospecting email on 24 June 2022.

First of all, with regard to your internal investigations, I have taken note that they revealed an "*error in the configuration of this procedure*" for the deletion of personal data, as your two databases, one relating to active customer accounts and the other dedicated to commercial prospecting, were not synchronised. Thus, the erasure measures implemented in the first were not automatically passed on in the second.

Then, with regard to the particular case of the complainant, I note that his customer account and the associated personal data were erased, upon receipt of his request in June 2022 and that his email address from the commercial prospecting database was manually deleted on 9 November 2022.

Finally, with regard to the measures taken to avoid the reiteration of such a situation, I note that an inventory of all erasure requests is in progress within your departments in order to identify any other cases that may have been impacted by this configuration error.

I also observe that measures to modify your internal procedure have been taken, in the short term, by replacing the current automatic procedure a request addressed to each of the departments in order to ensure the effective erasure of the personal data referred to in a request and, in the long term, by developing an automatic synchronization tool for all your databases.

RÉPUBLIQUE FRANÇAISE

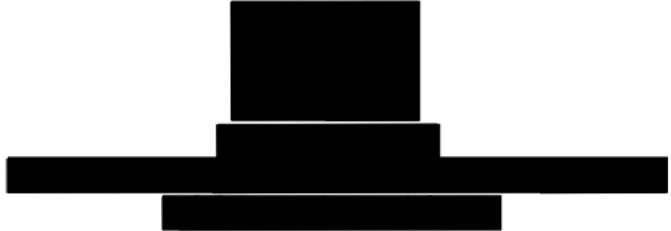
3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Consequently, the explanations given as to the circumstances of this incident and the measures already taken to avoid a repetition of the facts which are the subject of this complaint lead me, in agreement with the other European data protection authorities concerned by your processing operations, **to close it**.

However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and by the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,

For the CNIL Chair and on her behalf,



Copy to: [REDACTED] VP Legal & Compliance

[REDACTED]
[REDACTED]
CHIEF EXECUTIVE OFFICER
[REDACTED]
[REDACTED]

Investigation of the case:

Paris, on **10 MAI 2023**

Our Ref.: [REDACTED] CM [REDACTED]

Referral no. [REDACTED]
(to be quoted in all correspondence)

For the attention of the Chief Executive Officer,

I refer to the complaint sent by the data protection authority of the Land of Schleswig-Holstein in Germany pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

The complainant lodged a complaint with their national data protection authority against [REDACTED], a company established in France, concerning the information provided to data subjects on the website [REDACTED].

In particular, the complainant alerted his authority to the fact that [REDACTED] would not provide sufficient information concerning the processing of personal data implemented within the framework of its website [REDACTED]. In this respect, it appears that the website in question did not have an easily accessible privacy policy.

When queried regarding these factors, as part of the communications that took place between the CNIL departments and yourself, you adopted several measures to remedy this situation by:

- implementing a privacy policy easily accessible at the bottom of the home page of the website [REDACTED];
- translating it into several languages so that it can be accessed in all language versions of the website's home page;
- and by supplementing it to take into account the observations made by the CNIL in collaboration with the Schleswig-Holstein data protection authority.

RÉPUBLIQUE FRANÇAISE

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

As such, the measures implemented since September 2020 to inform internet users in accordance with Articles 13 and 14 of the GDPR led the CNIL, in agreement with the other European data protection authorities, **to close this complaint**.

However, please be aware that the CNIL reserves the right to make use of all the powers granted to it by the GDPR and by the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,

For the CNIL Chair and on her behalf,

A large rectangular black redaction box at the top, with a smaller horizontal redaction bar below it, centered vertically on the page.



Investigation of the case:

3rd July 2023

Our ref.: [REDACTED]

Referral no. [REDACTED]
(to be quoted in all correspondence)

Dear Mr Chairman,

I am following up on the emails that have been exchanged between the Commission nationale de l'informatique et des libertés (CNIL)'s departments (French Data Protection Authority) and the Data Protection Officer for [REDACTED] as part of the investigation into a complaint that was referred to us by the Swedish data protection authority in pursuance of Article 56.1 of the General Data Protection Regulation (GDPR).

The complaint concerned the difficulties that [REDACTED] had experienced in exercising his right to the erasure of his personal data with your company.

The complainant advised that he sent you a message on 6 December 2021 to request the deletion of his customer account, whose identifier was no. [REDACTED]. After asking him to confirm certain details of his account, your customer service department replied to him by email on 8 December 2021 and explained that his request had been transferred to the IT department to delete his account.

Since he had not received any confirmation that his account had been deleted as requested, [REDACTED] sent a new message to [REDACTED] on 8 January 2022. [REDACTED] replied in a message dated 10 January 2022 that its IT department was trying to delete his account, but since it was another department, there was no way to specify how long it would take to complete the procedure. [REDACTED] explained that he did not receive any subsequent confirmation from your company that his customer account had been deleted by your IT department.

I have noted that [REDACTED]'s request was taken into account from 8 December 2021, that he received confirmation by email on 15 February 2023 that his account had been deleted, and that your organisation's investigations were unable to explain the reason for such late confirmation, insofar as all his data have been deleted, and the only information currently in your possession relates to his request to exercise his right to erasure.

I also note that a reminder of the applicable procedure for managing data subjects' requests to exercise their rights has been sent to your customer service department to ensure that such requests are processed within the specified times.

Therefore, the answers provided by [REDACTED] lead me, in agreement with the other European data protection authorities concerned by your processing operations, to close this complaint.

However, in case of new complaints, the CNIL reserves the right to use all the powers vested by virtue of the GDPR and the French Data Protection Act no. 78-17 of 6 January 1978, as amended, relating to information technology, files and freedoms.

Yours faithfully,

For the CNIL Chair and on her behalf,

[REDACTED]
[REDACTED]
[REDACTED]

**Decision no. MED 2020-037 of November 12th, 2020 giving
order to comply to
the company [REDACTED]**

(Nº MDM201069)

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

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 the free movement of such data, in particular articles 56 and 60;

Having regard to Act no. 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act), particularly its article 20;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l'Informatique et des Libertés;

Having regard to decision no. 2019-041C of 15 February 2019 of the Chair of the Commission Nationale de l'Informatique et des Libertés tasking the Secretary General with performing or assigning a third party to perform an investigation on the company [REDACTED];

Having regard to records of investigation nos. 2019/041-1, 2019/041-2 and 2019/041-3 of 19 February, 20 February and 13 June 2019;

Having regard to the other items in the case file;

I. Context

[REDACTED] (hereinafter referred to as "the company") is a simplified joint-stock company located at [REDACTED].

The company belongs to the [REDACTED] Group, which is composed of three distinct companies: [REDACTED], a French holding company which wholly owns [REDACTED], an American company responsible for the Group's activities on USA territory and which itself wholly owns [REDACTED], the company forming the subject of this procedure. [REDACTED] was established in 2013 and the Group was established in 2015.

The company has about fifteen employees. [REDACTED] has four employees. [REDACTED] has about ten employees.

[REDACTED] is responsible for most of the Group's turnover. In 2018, its turnover was to the tune of [REDACTED]. It is currently in deficit. It carries out fundraising campaigns on a regular basis. It aims to be profitable in 2022.

In the context of its activity, [REDACTED] develops a mobile application (named [REDACTED], hereinafter referred to as “the application”) designed to put individuals into contact with one another in a professional context. A degraded version of the service is also accessible via a dedicated website. After completing a profile providing various items of personal information (including identity, position held, professional interests and goals), users are presented with the profiles of fifteen other members every day, mostly selected for their geographical proximity. Where there is mutual interest, individuals can contact each other on the application’s messaging service. Members can also subscribe to a service providing them with privileged access to a number of extra functionalities.

On 19 February 2019, pursuant to the Chair of the Commission’s decision no. 2019-041C of 15 February 2019, a CNIL delegation conducted an online investigation of the application published by the company. Onsite investigations on the company’s premises were carried out on 20 February and 13 June 2019.

In several exchanges of emails following the investigations, the company communicated various documents requested by the delegation, including accounting and contractual items.

On September 18th 2020, a draft decision was submitted to the concerned supervisory authorities as part of the cooperation procedure, on the basis of Article 60 of the GDPR.

This draft decision did not give rise to relevant and reasoned objections.

II. Characterisation of the facts

A breach of the obligation to minimise data

Article 5 of the GDPR provides that “*Personal data shall be [...] limited to what is necessary in relation to the purposes for which they are processed*”.

Firstly, the investigation delegation found that the application published by the company collects data on the geolocation of the device on which it is installed. The delegation was informed that these data were used to enable the company to present users with profiles of people living in the same city.

Yet the delegation also found that geolocation data was retained in the company’s servers with five decimal-place precision, which corresponds to a coordinate with one-metre accuracy. Collecting such accurate geolocation data would appear excessive as the profiles of people presented to users are located across a much wider area. The company could therefore provide an identical service by retaining degraded geolocation data.

Secondly, the investigation delegation was informed that a user using an Android device was obliged to provide a photograph when creating their account. Such obligation was not imposed on terminals operating on iOS or on the “browser” version of the service.

It would therefore appear that this piece of data is not necessary to the intended purposes of the published application and that nothing justifies it being required of users of terminals operating on Android.

Taken together, these facts constitute a breach of Article 5 of the GDPR as the company processes data not necessary to the intended purposes, including precise geolocation and the obligatory photograph for users of the Android device.

A breach of the obligation to set a data retention period proportionate to the purpose of the processing

Article 5 of the GDPR also provides that “*personal data shall be [...] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*”.

The delegation was informed that no retention period had been set for data stored in the company’s database, and those data are therefore retained with no limitation of duration.

As regards accounts whose creation procedure was not completed, the data already provided are retained with no limit set on duration. The delegation found that the company’s databases contained 428,905 accounts whose registration procedure had not been completed (out of a total of 1,916,379 registered accounts). One such uncompleted, inactive profile had been retained since its creation on 12 May 2016. Although data retention may be justified for a strictly determined limited period, in order to enable a user to complete an unfinished registration procedure, such retention is excessive beyond any retention period defined.

As regards accounts whose deletion has been requested by their users, the delegation found that they are assigned a special status and become unusable by the users concerned. However, the data are not erased from the database and are retained without justification on the part of the company.

As regards geolocation data, the delegation was informed that they are retained for sixty days and that each new position recorded is listed in the user’s geolocation history if it is more than five kilometres from any positions already recorded. If the new position is less than five kilometres from a position already recorded, the latter is incremented and the aforementioned sixty-day period is renewed. Each position records the date on which it was recorded for the first time as well as the incrementation number. The company’s database contains 761,834 positions recorded in user accounts. The delegation noted that a user’s account created in 2013 had been located over 17,000 times and that 73 positions connected with their profile had been retained. The investigation delegation also found that the position most frequented by the user concerned had been recorded on 18 November 2016 and incremented 1,709 times. Hence, the adopted system provides the company with extremely long visibility of presence in a given place when the user concerned regularly comes within the five-kilometre radius acting as reference. Retention of information on dates of creation of geolocation points is not necessary when retention of the date of its latest update is enough to achieve the desired objective.

As regards messages exchanged by members, the delegation was informed that all such messages were retained by the company. Hence, the delegation found that 30,453,795 messages were stored in the database. Although retention of messages exchanged by active users may be justified by the possibility provided to users of going back over the history of their exchanges, retention of messages exchanged by accounts that have become inactive or been deleted can only be regarded as excessive.

Taken together, these facts constitute a breach of Article 5 of the GDPR as data are retained for excessive periods given the purposes for which they were collected.

A breach of the obligation to inform data subjects

Article 13 of the GDPR obliges the data controller to communicate information to data subjects, including “*reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available*” when data is likely to be transferred outside the European Union (Article 13.1.f) and “*the existence of the right to withdraw consent*”

at any time" (Article 13.2.c). It also specifies that such information must be communicated to the data subject "*at the time when personal data are obtained*".

Article 12 of the GDPR obliges the data controller to ensure that such information is "*easily accessible*".

As regards content of the information, the delegation found that, when the application is opened, the homepage asks users to register or log on to their accounts. The homepage also includes two links, one to the general conditions of use and the other to the application's confidentiality policy.

The investigation delegation found that the confidentiality policy contained most of the information required by Article 13 of the GDPR, but no details of guarantees governing data transfer outside European Union territory; nor was the possibility of withdrawing consent included in the information notices, even though users' consent sometimes constitutes the legal basis of processing operations.

As regards accessibility of information, the delegation found that, although there was a link to the confidentiality policy on the homepage, there was no link enabling users to access the confidentiality policy and obtain communication of this information during the registration procedure, and therefore at the time when data are actually collected.

Taken together, these facts constitute a breach of Articles 12 and 13 of the GDPR as the information communicated by the company is incomplete and not accessible during collection of data.

A breach of the obligation to ensure data security and confidentiality

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

The delegation found that, when an account was created on the [REDACTED] application, a password composed of eight figures (in this case, "12345678") was accepted.

The delegation also found that the password protecting access to certain employees' workstations was only composed of eight characters comprising three of the four categories of characters. This is not complex enough, given that these workstations enable access to the company's database and that logins and passwords enabling connection are recorded in the database management software.

Authentication based on use of an insufficiently complex password may lead to associated accounts being compromised and to attacks by unauthorised third parties, brute-force attacks for example.

As an illustration, in its deliberation no. 2017-012 of 19 January 2017, the CNIL considered that, in order to meet password robustness requirements and ensure adequate levels of security and confidentiality, a password must contain at least twelve characters and include at least one uppercase letter, one lowercase letter, one figure and one special character. When a password is composed of eight characters, containing three of the four categories of characters, it must be accompanied by a complementary security measure (such as blocking the account after several unsuccessful attempts at connection) in order to ensure adequate levels of security and confidentiality.

Finally, the delegation was informed that passwords are stored in the database in the form of a hash obtained by the SHA-1 algorithm with addition of a salt.

In this respect, it should be borne in mind that the National Cybersecurity Agency of France's General Security Reference Framework advises against use of SHA-1, and has done so since it was first published in 2010 (Appendix B1 of General Security Regulation 1.20 of 26 January 2010, p. 24). Earlier versions of the reference framework for cryptographic mechanisms had already noted this hashing function's obsolescence since the update in 2008.

There must be no further use of cryptographic mechanisms based on the SHA-1 as it is no longer in keeping with the state of the art.

Taken together, these facts constitute a breach of Article 32 of the GDPR as access to application users' accounts and to developers' workstations is not protected by passwords of a complexity appropriate to the data protected and as the algorithm used for hashing users' passwords uses a hashing function with known vulnerabilities.

Failure to access, by means of electronic communication, information already stored on the user's terminal without the user's consent and without specific information.

Article 82 of Act no. 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act) provides that : “*Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by the data controller or its representative, except if already previously informed, regarding:*

1° the purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in this device;

2° the means available to them to object to such action.

Such access or recording may only be carried out provided that the subscriber or user has explicitly expressed, after receiving said information, their agreement that may result from appropriate parameter settings in their connection device or any other system under their control.”

The same article specifies that obtaining the consent is not mandatory when the access to data is “*either exclusively intended to enable or facilitate communication by electronic means” or “strictly necessary for the provision of an online communication service at the user’s express request”.*

When installing the application and creating an account, the inspection delegation found that the user was asked to allow the application to access the position of the device used via GPS through a pop-up window generated by the phone system. If the user refuses to give access to his or her geolocation data, he or she is redirected to an application page that requests again access to the data with a single button entitled “*Give access to my position*”. The pop-up window reappears when the user clicks on this button. Then, if the user refuses to share his geolocation data again, he or she is redirected to the application page previously mentioned, must click on “*Give access to my position*”, and is again asked to allow the application to access the position through the pop-up window. The user can only continue the registration process by clicking on the “*Allow*” button in the window.

These elements show that the user is forced to share his geolocation data in order to register and use the application from his mobile phone.

The delegation was informed that providing geolocation data was mandatory in the mobile versions of the application, whereas users of the service's web interface had to manually enter their location to be offered nearby profiles. It can be deduced that the geolocation data of the user's device is not strictly necessary for the provision of the service, since other solutions are offered on other platforms of the application, such as manual activation. Moreover, providing the geolocation data is not exclusively intended to enable communication.

Therefore, the consent of the user had to be obtained prior to the collection of the data.

However, article 2 of the French Data Protection Act provides that "*except where otherwise provided, within the framework of this Act, the definitions of Article 4 of Regulation (EU) 2016/679 of 27 April 2016 shall apply*".

Article 4.11 of GDPR defines the consent 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*".

In this case, as long as the offered service does not require access to geolocation data, the user should be able to refuse to give his or her consent without being denied access to the service from a mobile phone, as it is allowed on the web interface. Such consent is not free and cannot be considered as valid within the meaning of the GDPR and the French Data Protection Act.

Therefore, these facts constitute a breach of Article 82 of the French Data Protection Act since the user does not validly consent to access his or her geolocation data on his or her terminal.

In light of the above, the company [REDACTED] located at [REDACTED], is hereby given order to comply, within 5 (five) months from the notification of this decision and subject to measures it may already have adopted, to:

- **collect adequate, relevant data limited to what is necessary in view of the purposes for which they are processed**, in particular, unless its necessity can be justified, stop collecting the user's geolocation with one-metre accuracy and stop obligatory collection of users' photographs during creation of profiles;
- **define and implement a policy on user data retention periods that do not exceed the periods necessary to the purposes for which they are collected**, in particular regarding data on users who have not completed the account creation procedure and geolocation data;
- **inform data subjects in compliance with the provisions of Articles 12 and 3 of the Regulation, with regard to personal data processing carried out**, and, in particular, provide information on the legal basis for such processing and a full description of data subjects' rights, and ensure provision of all the information referred to in Article 13 of the du GDPR, either on the registration form or via a link on the form;
- **for all personal data processing operations implemented, take all necessary measures to enable maintenance of such data's security and prevent unauthorised third parties accessing them**, in particular:

- by storing passwords transformed by means of a reliable non-reversible cryptographic function (i.e. using a public algorithm deemed to be strong whose software implementation has no known vulnerabilities) such as SHA-256;
- by implementing a binding policy on passwords used by users of the sites and mobile applications operated by the company, in line, for example, with one of the following modalities:
 - passwords composed of at least 12 characters, containing at least one uppercase letter, one lowercase letter, one figure and one special character;
 - passwords composed of at least 8 characters, containing 3 of the 4 categories of characters (uppercase letters, lowercase letters, figures and special characters) and accompanied by a complementary measure such as delaying access to an account after several failures, inclusion of a mechanism protecting against intensive automated attempts (e.g. “captcha”) and/or blocking the account after several unsuccessful attempts at authentication (10 at most);
- **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 order to comply, 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 order to comply, a rapporteur shall be appointed and may request that the restricted committee issue one of the penalties set out under Article 20 of the Act of 6 January 1978, amended.

The Chair

Marie-Laure DENIS

**Decision no. MED 2020-041 on November 24, 2020, issuing formal notice to
the company [REDACTED]**

(N°MDM201040)

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 the free movement of such data, in particular articles 56 and 60;

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 liberties (French Data Protection Act), particularly its article 20;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l’Informatique et des Libertés;

Having regard to decision no. 2019-083C of 24 April 2019 of the Chair of the Commission Nationale de l’Informatique et des Libertés tasking the Secretary General with performing or assigning a third party to perform an investigation on the [REDACTED] and [REDACTED], subsidiaries of the [REDACTED];

Having regard to records of investigation nos. 2019-083/1 of 6 August 2019 and 2019-083/2 of 7 August 2019;

Having regard to the complaints no. 18007540, 18009275, 18021587, 18024134, 19000332, 19000605, 19001259, 19004708, 19006278, 19008043;

Having regard to the other items in the case file;

I. The procedure

The single-shareholder simplified joint-stock company [REDACTED] (hereinafter “the company”), a subsidiary of the [REDACTED], operates as an affinity insurance broker, mainly for telephone and multimedia products. It has approximately 800 employees. Its registered office is located at [REDACTED].

During 2018 and 2019, the Commission was referred to regarding several complaints made by customers and prospects stating that the company had not complied with their rights to access, object to and erase their personal data.

Pursuant to the Chair of the Commission nationale de l'informatique et des libertés' (hereinafter the "CNIL") decision no. 2019-083C, a CNIL delegation conducted two on-site investigations on 6 and 7 August 2019 regarding the [REDACTED], with a view to verifying the compliance of the personal data processing carried out by the latter.

In this context, the company informed the delegation that it conducts telephone and email marketing campaigns to sell its insurance policies using prospect lists purchased from its partners, which are mainly companies specialised in the collection and sale of prospects' data and companies distributing telephone or multimedia products. To date, around two million individuals are said to be concerned by the company's marketing activities.

The company subsequently provided the delegation, by email, with additional documents requested as part of the investigation relating, in particular, to the number of prospect personal data files purchased by the company, copies of marketing emails sent by the company, the methods used to verify the validity of prospects' consent to receiving marketing emails collected by the company's partners.

On September 22, 2020, a draft decision was submitted to the concerned supervisory authorities as part of the cooperation procedure, on the basis of Article 60 of the GDPR.

This draft decision did not give rise to relevant and reasoned objections.

II. The breaches

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

Pursuant to Article L. 34-5 of the Postal and Electronic Communications Code, "*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*". The same article also provides that "*consent shall be understood as any free, specific and informed indication of the data subject's wishes by which he/she accepts that his/her personal data be used for marketing purposes*".

Furthermore, Article 4. 11) of the Regulation defines consent as "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

Lastly, Article 7.2. of the Regulation provides that "*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*". As a result, the data subject should be able in theory to give their consent independently and specifically for each distinct purpose.

The delegation was informed and found that the company conducted email marketing campaigns to sell its insurance products using prospect lists purchased from its different partners.

The company informed the delegation that its partners are contractually required to provide it with prospect lists containing the data of individuals having consented to their data being transferred to partners. Data subjects' consent is therefore collected by the provider of the prospect list.

However, the delegation found that partner companies [REDACTED], [REDACTED], [REDACTED] and [REDACTED] collect data subjects' consent using only one box to be ticked on a consent form relating to at least two separate processing of personal data: participation in a competition and consent to receiving marketing messages from partners.

Therefore, data subjects' consent to the use of their data for marketing purposes by the contracting third parties is not collected in accordance with applicable provisions.

Thus, even though the company does not collect itself data prospects' consent, the company could not conduct marketing campaigns targeting data subjects appearing in the prospect list bought from partner companies [REDACTED], [REDACTED], [REDACTED] and [REDACTED], since then the data subjects' consent had not been validly collected.

By conducting marketing campaigns targeting data subjects whose consent to receive marketing messages had not been validly collected, the company acted in breach of the provisions of Article L. 34-5 of the Postal and Electronic Communications Code and of Articles 4 and 7 of the Regulation.

A breach of the requirement to provide proof that consent was given by the data subject

Article 7.1. of the Regulation provides that "*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his/her personal data*".

The delegation found that the company's partners are responsible for collecting data subjects' consent to the processing of their personal data for marketing purposes.

The delegation was also informed and found that, when a prospect disputes that their consent has been collected, a request is sent to the provider of the file to ensure consent has indeed been given and an audit of the process to collect consent is conducted by the partner.

The company was therefore able to provide the delegation with documents, such as the consent collection forms presented by partner companies to their customers, enabling to establish, in general, the process implemented by its partners to collect prospects' consent. The delegation was further informed that a tool had been introduced in 2018 to track the origin of prospect lists. This tool provides the origin of each prospect and provides the prospect with information when requested.

However, the delegation found that the verification process implemented by the company in respect of its partners does not enable it to ensure that consent has indeed been given individually by each of the prospects.

Thus, the company is not able to prove that each of the individuals targeted by its marketing campaign have indeed given their consent to the processing of their data.

These actions are in breach of article 7.1 of the GRPD.

A breach of the requirement to inform data subjects

Article 13 of the GDPR requires that, at the time when data are obtained, the data controller provides information relating to its identity and contact details, the contact details of the data protection officer, the purposes of the processing and its legal basis, the recipients of the personal data, where applicable the transfer of personal data, the period of storage of the data, the rights of data subjects and the right to lodge a complaint with a supervisory authority.

However, the delegation was informed and found that, when recording telephone conversations, the script followed by telesales personnel does not provide for the complete information of prospects. By listening to a sample of telephone conversations held, the delegation noted that, while the individuals contacted are indeed informed of the principle of recording, they are not, however, informed of the rights that they possess, and in particular of their right to object to the recording of their telephone conversation.

These actions are in breach of the requirement to inform data subjects pursuant to Article 13 of the GDPR.

A breach of the requirement to keep a complete record of processing activities

Article 30 of the Regulation provides that a data controller enterprise employing fewer than 250 persons is required to hold a record of processing activities when its personal data processing is not occasional.

In this case, the record of processing activities must contain all information listed under Article 30.1 of the GDPR, i.e.: the name and contact details of the controller, its representative and the data protection officer, the purposes of the processing, the categories of data subjects and the categories of personal data, where applicable the transfers of data and where possible the envisaged time limits for erasure of data and a description of the technical and organisational measures implemented to ensure a certain level of data security based on the risk.

The delegation found that the processing of prospects' and customers' data is part of the company's usual activity, which requires that it hold a record of processing activities in compliance with the provisions of Article 30 of the Regulation.

While the delegation found that the company does keep a record of processing activities, said record does not contain all the information required by Article 30 of the Regulation. In particular, the record does not contain information on:

- the categories of personal data processed;
- the envisaged time limits for the erasure of the different categories of data;
- the categories of data subjects concerned by the processing.

Thus, these actions are in breach of the requirements set out by Article 30 of the Regulation.

In light of the above, the company [REDACTED], located [REDACTED], is hereby given formal notice, within three (3) months from the notification of this decision and subject to measures it may already have adopted, to:

- **stop conducting marketing operations targeting individuals whose consent has not been validly collected, particularly by its partners [REDACTED], [REDACTED], [REDACTED] and [REDACTED],**

- **be able to demonstrate, for each data subject, that their consent to the processing of their personal data by the company for marketing purposes has indeed been collected in advance by its partners**, for example by systematically requiring that partners provide full information on the means and conditions under which consent is collected, in particular the date on which consent is collected, on the physical point of sale or the website on which consent was given and on the product or competition concerned,
- **inform data subjects** in accordance with the provisions of Article 13 of Regulation (EU) by completing the information provided to prospects by telephone, notably on their right to object to the recording of their conversation,
- **hold a record of processing activities containing all required indications**, including the categories of data subjects and the personal data processed as well as the period of storage of such data.
- **justify, to the CNIL, compliance with all of the above requests within the time-limit set.**

After this time-limit, if the company █ 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 █ has not complied with this formal notice, a rapporteur shall be appointed and may request that the restricted committee issue one of the penalties set out under Article 20 of the Act of 6 January 1978, amended.

The Chair

Marie-Laure Denis

Summary Final Decision Art 60

Complaint

Compliance order

EDPBI:FR:OSS:D:2020:164

Background information

Date of final decision:	24 November 2020
Date of broadcast:	4 December 2020
LSA:	FR
CSAs:	BE, ES
Legal Reference:	Conditions for consent (Article 7), 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), Records of processing activities (Article 30)
Decision:	Compliance order
Key words:	Advertising, Consent, Consumer protection, Data subject rights, Direct marketing, E-commerce

Summary of the Decision

Origin of the case

Customers and prospects filed complaints against the controller, claiming that the controller did not comply with its obligations to ensure the right to access, the right to object and to erase their personal data. The company at issue is conducting telephone and email marketing campaigns to sell insurance policies using prospect lists purchased from its partners. To date, these marketing activities reached around two million individuals.

Findings

The LSA found that the controller's partner companies collected data subjects' consent to use of their data for marketing purposes by the third parties using only one box to be ticked for at least two separate processing of personal data: participation in a competition and consent to receiving

marketing messages from partners. Moreover, the LSA concluded that the controller is not able to prove that each of the individuals targeted by its marketing campaign has given individually their consent. The LSA found that the controller, contacting individuals by phone, did not inform them about their rights, in particular the right to object. In addition, the LSA found that although the controller keeps record of its processing activities, the record lacks some obligatory information.

Therefore, the LSA found that the controller acted in breach of Articles 4(11), 7(1), 7(2), 13 and 30 GDPR.

Decision

The LSA gave a formal notice to the controller.

Within three (3) months from the notification of the decision, the controller was ordered to: stop conducting marketing operations targeting individuals whose consent has not been validly collected; be able to demonstrate that the data subject's consent has indeed been collected in advance by the controller's partners; fully inform the data subjects in accordance with Article 13 GDPR; hold a record of processing activities containing all required indications; justify compliance with all of the above requests within the deadline.

Summary Final Decision Art 60

Investigation

Compliance order, Administrative Fine, Publication of the controller's name

EDPBI:FR:OSS:D:2020:134

Background information

Date of final decision:	28 July 2020
Date of broadcast:	11 August 2020
LSA:	FR
CSAs:	AT, BE, BG, HR, CY, CZ, DK, DE, EE, EL, FI, HU, IE, IT, LV, LT, LU, MT, NL, PL, PT, RO, SK, SI, ES, SE, UK
Legal Reference:	Principles relating to processing of personal data (Article 5), Security of processing (Article 32), Transparency and Information (Articles 12, 13 and 14)
Decision:	Compliance order, Administrative Fine, Publication
Key words:	Data minimisation, Storage limitation, Transparency, Employees, Clients, E-commerce, Data security.

Summary of the Decision

Origin of the case

The controller conducted full and permanent recording of all phone calls from its customer service employees, and without their ability to object. The controller did not prove that it had limited this processing to what is necessary for the purposes of assessing and training its employees. The controller also recorded the bank details of customers placing orders by telephone when recording its employees' conversations for training purposes and stored such data in clear text in its database for fifteen days.

The controller collected copies of Italian health cards and valid identity cards for anti-fraud purposes.

The controller also stored a significant amount of personal data of customers who had not connected to their account in over ten years and of individuals that had never placed an order on the company's website. After the expiry of the storage period for customers' data, the company keeps some of their data such as their e-mail address, and password in pseudonymised form for the alleged purpose of enabling customers to reconnect to their accounts.

The controller did not inform its customers that their data were transferred to Madagascar. The controller only cited in its privacy policy one legal basis for processing: consent whereas it conducted several processing operations on different legal basis. The controller did not inform either its employees individually of the recording of their telephone calls.

The controller accepted to log into user accounts passwords comprised of eight characters and only one category of characters. It also requested its customers to provide it with a scan of the bank cards used on ordering for anti-fraud purposes, which were subsequently stored by the company in clear-text and containing all of the credit card numbers for six months.

Findings

The LSA considered that the controller's recording of all phone calls from its customer service employees, including the bank details of customers placing orders by telephone and the collection of Italian health cards, which contain more information than the identity card that is not relevant to combat fraud, was excessive and concluded that it was a breach of the data minimisation principle of Article 5.1.c. GDPR.

The LSA concluded that the company's storage of a significant amount of personal data of former customers and prospects over long periods that exceed the purposes for which data were processed violated the storage limitation principle of Article 5.1.e. GDPR.

The LSA considered that the controller had not informed customers up to a specific date of the transfers of data to Madagascar, provided for each processing operation the corresponding legal basis in its privacy policy and adequately informed its employees of the recording of their telephone calls. All these failings constituted a breach of Article 13 GDPR (information provided to data subjects).

The LSA considered that the company did not take sufficient security measures to ensure the security of its customers' bank data, which violated Article 32 GDPR (security of processing).

Decision

The LSA decided to impose a compliance order on the controller to remedy its breaches of the principles of data minimisation, data storage limitations, requirement to inform data subjects, and to ensure data security. It associated the compliance order with a periodic penalty payment of 250 euros per day of delay on expiry of a period of 3 months following the notification of this decision.

The LSA also imposed on the controller an administrative fine of 250,000 euros.

The LSA further decided to make its decision public on its website, identifying the company by name, for a period of two years.

**Decision no. MED 2021-007 of 28 January 2021 issuing an order to comply
to [REDACTED]**

(N° MDM211005)

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

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 the free movement of such data, particularly its articles 56 and 60;

Having regard to Act no. 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act), particularly its article 20;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l’Informatique et des Libertés;

Having regard to decision no. 2019-080C of 7 May 2019 of the Chair of the Commission Nationale de l’Informatique et des Libertés tasking the Secretary General with performing or assigning a third party to perform an investigation on all processing of personal data, bearing whole or partially on data relating to the marketing and use of products and services attached to the [REDACTED] product, and encompassing all organisations concerned in their impleme

Having regard to records of investigation nos. 2019-080/1 of 20 June 2019, 2019-080/2 of 4 July 2019 and 2019-080/3 of 1 August 2019;

Having regard to the other items in the case file;

I. The procedure

[REDACTED] (hereinafter “the company”), located at [REDACTED], is a simplified joint-stock company established in 2016. The [REDACTED] and recorded a turnover of around 670,000 euros in 2018, with a negative result of 40,000 euros.

The company markets the [REDACTED] children’s smart watch, which, via the mobile application published by the company, enables parents to view the geolocation of children wearing the smart watch in real time, send them voice messages, and predefine delimited areas which the children are not authorised to leave.

The company markets the [REDACTED] in France via its website [REDACTED], which also has English, Spanish and German extensions, and in the United Kingdom, Spain and Germany via Amazon’s website.

Pursuant to decision no. 2019-080C of 7 May 2019 of the Chair of the Commission Nationale de l’Informatique et des Libertés (the French Data Protection Commission, hereinafter the “CNIL”), a CNIL delegation carried out two online investigations on 20 June 2019 and 1 August 2019, and an onsite investigation at [REDACTED] on 4 July 2019.

These investigations focused largely on information brought to data subjects’ knowledge as regards processing of personal data carried out by the company, obligations relating to subcontracting, and the obligation to ensure data security.

On 8 October 2020, in the context of the cooperation procedure, a draft decision has been submitted to the supervisory authorities concerned on the ground of article 60 of the Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016.

This draft decision has not given rise to any relevant and reasoned objections.

II. **Breaches**

A breach of the obligation to inform data subjects of the processing of their data

Articles 12 and 13 of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (hereinafter referred to as the “GDPR” or “Regulation”) require the data controller to provide data subjects with full information on the processing implemented, and do so in “*concise, transparent, easily intelligible*” fashion.

Firstly, the delegation found that the information provided to the purchaser of a [REDACTED] [REDACTED] smart watch using the [REDACTED] mobile application is incomplete as it does not contain all the points provided for in Article 13 of the GDPR.

First of all, the **general conditions** of use available on the [REDACTED] website and the [REDACTED] mobile application do not contain all the information provided for in Article 13 of the GDPR. Although the general conditions of use identify the data collected (including name, physical address, IP address, email address and geolocation data) and state that they are used “*for the sole purposes of creating the functionalities expected of [REDACTED] SAS Software and monitoring commercial relations with users, for security purposes in compliance with the applicable laws and regulations and to enable improvement and personalisation of the products and services provided to users and the information communicated to them*”, they do not specify the legal basis for their processing, the data retention period or at the very least the criteria used to determine such period, or make mention of the existence of the right to limitation and portability of data or the right to make a complaint to a supervisory authority.

The same is true of the **confidentiality policy**, acceptance of which is required for creating an account on the [REDACTED] mobile application. Although the delegation found that the confidentiality policy informs [REDACTED] mobile application users that their personal data is processed by [REDACTED] in order to provide and improve the service, and in particular to “*process your orders, comply with legal procedures, respond to emergencies, develop and inform you of new products and services, monitor, assess and improve our products, services, systems and networks, and personalised your experience with our services*”, it contains no information on the legal basis for the processing, the data retention period or at the very least the criteria used to determine such period, or make mention of the existence of

the right to limitation and portability of data, the existence of the right of objection, access, rectification and erasure (only in the case of the confidentiality policy) or the right to make a complaint to a supervisory authority.

Secondly, the delegation found that the information provided by the company in its confidentiality policy and general conditions of use is not concise or easily intelligible within the meaning of Article 12 of the GDPR.

First of all, the confidentiality policy lacks clarity. Its titles tend to be ambiguous and repetitive (“*collection and use of information*”, “*use of personal information*”, “*authorisations*”) and are not clearly prioritised due to lack of graphic consistency: some titles are in bold, while others are underlined.

Furthermore, information on one and the same subject is scattered among several sections, in particular as concerns data recipients, thus hampering its intelligibility.

Finally, the confidentiality policy contains a great deal of vague, generic wording, e.g. “*we may share personal and non-personal information with affiliated entities for approved business purposes*” or “*we may access, monitor, use or divulge your personal information and communications in order to do such things as: (...) protect the rights and property of ourselves, our employees, our members, our customers and other persons, (...) respond to emergencies, launch, provide, invoice and receive services (...)*”. The same is true of the general conditions of use, which, for example, state that data collected are used “*for the sole purposes of creating the functionalities expected of [REDACTED] SAS software*” without it being possible for users to determine the functionalities provided by the smart watch involve processing of personal data.

This results in the user being unable to fully understand the way their personal data is processed by [REDACTED]

Taken together, these facts constitute a breach of Articles 12 and 13 of the GDPR, which require the data controller to provide, at the time the data are collected and in “*concise, transparent, intelligible and easily accessible*” fashion, information on the legal basis for the processing, recipients of personal data, the personal data retention period and data subjects’ rights.

A breach of the obligation to have processing operations carried out on behalf of the data controller governed by a formal legal act

Article 28 of the GDPR provides that processing carried out by a processor on behalf of a data controller must be governed by a contract that sets out the conditions under which the processor undertakes to carry out processing operations on behalf of the data controller, and also contains information on the controller’s obligations and rights.

The delegation was informed that [REDACTED] subcontracted the processing of [REDACTED] smart watches’ geolocation data to the company [REDACTED] for the purpose of displaying weather forecasts on the watch.

The delegation found that the contract concluded between [REDACTED] and [REDACTED] did not contain the clauses provided for by Article 28 of the GDPR.

These facts constitute a breach of obligations of Article 28 of the Regulation.

A breach of the obligation to ensure the security of personal data

Article 32 of the GDPR requires the data controller to ensure a level of security of the processing it carries out appropriate to the risks involved.

On the absence of encryption of communications

During the onsite investigation of 4 July 2019, the delegation was informed that all requests sent to the [REDACTED] server by the application and the smart watch are in non-secure “http” format.

Yet a connection via a non-secure channel makes all information exchanged vulnerable, including the identifiers and passwords enabling connection to the tool.

The data controller should therefore encrypt the channel used for all requests sent to the [REDACTED] server by the application and the smart watch in order to protect the confidentiality of data so exchanged.

On the absence of authentication of requests

The online investigation of 1 August 2019 showed that the company has not implemented a system for authentication of communications between the application and the server.

As a result, the origin and authenticity of requests are not guaranteed, which results in a risk of identity theft and access to data by unauthorised individuals.

It is therefore the company’s responsibility to implement a system ensuring authentication of requests between the [REDACTED] application and the [REDACTED] sever (by means of a TLS protocol, for example) as the server only accepts legitimate requests, i.e. coming from known users of the server who have right of access to various of its resources.

On inadequate security of passwords

Firstly, the investigation delegation found that the data controller had taken measures to ensure that very simple passwords were refused, both during creation of a user account in the [REDACTED] application and during employees’ connection to the database containing data collected by [REDACTED] smart watches.

Although such measures may be regarded as best practices, in this case they proved to be inadequate. As regards users, the delegation found that a password composed of nine characters with two types of characters was accepted when an account was created, with no complementary measure such as blocking the account after several unsuccessful attempts at connection. Likewise, as regards employees’ access to the database containing data collected by [REDACTED] smart watches, the delegation was informed that a password composed of eleven characters with four types of characters was accepted, with no complementary measure such as blocking the account after several unsuccessful attempts at connection.

Yet authentication based solely on use of an inadequately robust password may lead to associated accounts being compromised and attacks by unauthorised third parties, brute force for example. The processing carried out by the [REDACTED] application and the [REDACTED] server makes data identifying minors accessible, so carrying a major risk for data subjects in the event of illegitimate access to such data.

As an illustration, in its deliberation no. 2017-012 of 19 January 2017, the CNIL considered that, in order to meet password robustness requirements and ensure adequate levels of security and confidentiality, a password must contain at least twelve characters and include at least one uppercase letter, one lowercase letter, one figure and one special character. When a password is composed of eight characters, containing three of the four categories of characters, it must be accompanied by a complementary security measure (such as blocking the account after several unsuccessful attempts at connection) in order to ensure adequate levels of security and confidentiality.

Secondly, the delegation was informed that no password renewal policy had been implemented.

Thirdly, the delegation found that the [REDACTED] application account's password hashing algorithm used in the database and the password modification URL is the MD5 algorithm, which is now deemed obsolete in terms of security insofar as it has widely known vulnerabilities that make it easily reversible in the event of passwords being divulged in their hashed form.

On lack of traceability of accesses

The delegation was informed that access to the base containing data collected by [REDACTED] smart watches was via a "root" account (an account possessing the system's highest level of rights) shared by two of the company's employees.

Allowing two technicians to share an account giving access to the database containing data collected by [REDACTED] smart watches is a practice that does not reliable authentication of users and, in consequence, makes management of authorisations and traceability of accesses and individual actions impossible. Such lack of traceability also makes it impossible to identify individuals gaining fraudulent access to, damaging or erasing data.

These facts go to show that the security measures implemented do not ensure an adequate level of security of the personal data processed and that they therefore constitute a breach of obligations of Article 32 of the Regulation.

In light of the above, the company [REDACTED], located [REDACTED], is hereby given an order to comply, within six (6) months from the notification of this decision and subject to measures it may already have adopted, to:

- **inform the individuals from whom personal data is collected, in compliance with the provisions of Articles 12 and 13 of the GDPR**, in particular by providing them with full, easily intelligible information on the legal basis for the processing, personal data recipients, data retention periods or at the very least the criteria used to determine such periods, the existence of the right to limitation and portability of data, the existence of the right of objection, access, rectification and erasure (only in the case of the confidentiality policy) and the right to make a complaint to a supervisory authority;
- **make additions to the contract** concluded between [REDACTED] and [REDACTED] so that it includes all the in article 28-3) of Regulation (EU) 2016/679;

- **for all personal data processing operations implemented, take all necessary security measures to enable maintenance of such data's security and prevent unauthorised third parties accessing them**, in particular:
 - by encrypting the channel used for connection to the production database, e.g. by using the HTTPS protocol;
 - by implementing a system ensuring authentication of requests between the [REDACTED] application and the [REDACTED] server, and only authorising those that are legitimate (e.g. by means of a TLS protocol);
 - by implementing a binding policy on passwords, in particular in terms of complexity, in line with the following modalities:
 - passwords composed of at least 12 characters, containing at least one uppercase letter, one lowercase letter, one figure and one special character; or
 - passwords composed of at least 8 characters, containing 3 of the 4 categories of characters (uppercase letters, lowercase letters, figures and special characters) and accompanied by a complementary measure such as delaying access to an account after several failures, inclusion of a mechanism protecting against intensive automated attempts (e.g. “captcha”) and/or blocking the account after several unsuccessful attempts at authentication (10 at most);
 - by providing for renewal of passwords (every six months, for example);
 - by ensuring that each technician logs on to the base containing data collected by [REDACTED] smart watches using their own individual identifier and password;
- **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 order to comply, 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 order to comply, a rapporteur shall be appointed and may request that the restricted committee issue one of the penalties set out under Article 20 of the Act of 6 January 1978, amended.

The President

Marie-Laure DENIS

Deliberation of restricted committee no. SAN-2021-001 of 6 January 2021 concerning

The *Commission nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Authority), met in its restricted committee composed of Alexandre LINDEN, chairman, and Anne DEBET, Sylvie LEMMET and Christine MAUGÜE, members;

Having regard to Council of Europe Convention No. 108 of 28 January 1981 for the protection of persons with regard to the automated 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 amended French Data Protection Act no. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to decree no. 2019-536 of 29 May 2019 implementing law no. 78-17 of 6 January 1978 on data protection;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the rules of procedure of the CNIL (French Data Protection Authority);

Having regard to decision no. 2019-42C of 15 February 2019 of CNIL's chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing implemented by that organisation or on behalf of [REDACTED];

Having regard to the decision of CNIL's chair appointing a rapporteur before the restricted committee of 27 January 2020;

Having regard to referral PL19000723 received by the CNIL on 9 January 2019;

Having regard to the report of [REDACTED], the commissioner rapporteur, notified to [REDACTED] on 24 February 2020;

Having regard to the written observations made by [REDACTED] on 23 March 2020;

Having regard to Order no. 2020-306 of 25 March 2020 on the extension of the deadlines due during the health emergency period;

Having regard to the rapporteur's response to these observations notified on 22 April 2020 to the company's board;

Having regard to the written observations of [REDACTED] received on 20 August 2020 and the oral observations made at the restricted committee meeting;

Having regard to the other documents in the file;

At the restricted committee meeting of 10 September 2020, which was partially held by videoconference the following were present:

- [REDACTED], commissioner, heard in his report;

In the capacity of representatives of [REDACTED]:

- [REDACTED], lawyer at the Paris Bar;
- [REDACTED], [REDACTED] (by video conference);

As a representative of [REDACTED]:

- [REDACTED] (by video conference);

[REDACTED] having last spoken;

The restricted committee adopted the following final decision:

I- Facts and proceedings

1. [REDACTED] (hereinafter "the company") is a simplified joint-stock company founded in France in [REDACTED], specialising in optical retail trade and whose registered office is located at [REDACTED]. For this purpose, it has around 100 branches, mostly located on French territory, as well as a network of approximately 450 franchise stores worldwide.
2. In 2017, [REDACTED] achieved a turnover of [REDACTED] and more than [REDACTED] in profits.
3. The company also publishes, for the purposes of its activity, the [REDACTED] (hereinafter the "company website"), which allows its customers to make online orders. Other variations in this site target consumers in Germany ([REDACTED]), Spain ([REDACTED]) and the United Kingdom ([REDACTED]).
4. On 4 January 2019, the company sent to the French Data Protection Authority (hereinafter the "CNIL" or the "Authority") a notification relating to an "*attack on the Internet sales website of [REDACTED] by a hacker*" which resulted in a "*probable intrusion on the servers hosting the site*".
5. In a letter supplementing the notification sent to CNIL on 11 January 2019, the company indicated that the intrusion had compromised the personal data of 210,692 customers. After analysis, it was established that the customers of the company concerned are mainly French but also include European nationals and third-country nationals. The personal data displayed on this occasion are the email address, hash of the user account's password, the first and last names, address, telephone number, date of birth of the data subjects and, for 23,000 of them, the social security number.
6. On 19 February 2019, pursuant to CNIL chair's decision no. 2019-42C, a CNIL delegation carried out an audit at the premises of [REDACTED]. The purpose of this audit was to verify compliance by this company with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the Regulation" or

"GDPR") and with the amended law no. 78-17 of 6 January 1978 on data protection (hereinafter "the amended law of 6 January 1978" or "the French Data Protection Act") by examining in particular the circumstances of the aforementioned personal data breach.

7. During this audit, the delegation was informed that the website [REDACTED] is published by [REDACTED], but that its development, administration and security had been carried out since 2013 by a provider, [REDACTED], established in Israel.
8. With regard to the unfolding of the personal data breach, the delegation was informed, in particular, that on 26 December 2018, attackers had exploited a vulnerability affecting the jQuery-File-Upload module that the company is deploying on its website to enable the uploading of its customers' orders to their user account. The exploitation of the vulnerability of this module allowed attackers to place files on the web server containing the tools necessary to extract personal data from this server. On 27 December 2018 and on 2 January 2019, [REDACTED] detected abnormal files on the web server, which it deleted the same day.
9. On 3 January 2019, after discovering a new intrusion into the servers of the website, [REDACTED] informed the controller of the situation. In order to permanently cut off the attack, the two companies decided to use [REDACTED], specialising in information systems security auditing, which sent them its intervention report on 10 January 2019.
10. Following these events, [REDACTED] and [REDACTED] took various measures to put an end to the attack and avoid it being repeated. Both companies implemented the recommendations made by [REDACTED], such as updating the vulnerable module with the latest available version, removing unnecessary or compromised files and folders at the root of the site, changing the SSH key, i.e. the secure communication protocol used to connect to the web server, and strengthening the security measures governing the connection of a customer to its user account.
11. On 29 April 2019, a CNIL delegation carried out an online audit on the [REDACTED] website, in order to verify the compliance of the processing of personal data implemented by [REDACTED] and in particular the aforementioned website.
12. On 27 and 28 May 2019, an auditing delegation arrived at the premises of the company's registered office. This second on-site audit, which was part of the investigation of several complaints from customers or prospects of the company received by CNIL, particularly concerned commercial prospecting and the exercise of personal rights.
13. In emails received between March and September 2019, the company sent the CNIL various documents requested by the delegation as part of these three audits, such as the contractual documents binding the company to several of its service providers, including [REDACTED], as well as the company's exchanges with the customers responsible for the complaints received by the Authority. The company also provided CNIL, by email dated 15 November 2019, with the new "*Personal Data Charter*" posted on its website.

14. In order to examine these items, the chair of the Authority appointed [REDACTED] as rapporteur, on 27 January 2020, on the basis of Article 22 of the amended law of 6 January 1978.
15. In accordance with Article 56 of the GDPR, on 18 February 2020 the CNIL informed all European supervisory authorities of its competence to act as the lead supervisory authority concerning the cross-border processing carried out by the company and opening the procedure for the declaration to the relevant authorities in this case.
16. At the end of his investigation, the rapporteur had a bailiff notify [REDACTED], on 24 February 2020, of a report detailing the breaches of the GDPR that he considered constituted in this case.
17. This report proposed to the Authority's restricted committee to pronounce an injunction to bring the processing into line with the provisions of Article 12(2) and Article 32 of the Regulation, accompanied by a penalty at the end of a period of three months following notification of the decision of the restricted committee, as well as an administrative fine.
18. Also attached to the report was a notice to attend the restricted committee meeting on 30 April 2020 indicating to the company that it had one month to provide its written observations in response to the report.
19. On 4 March 2020, the company made a request for the restricted committee meeting to be held behind closed doors.
20. In a letter dated 10 March 2020, the chairman of CNIL's restricted committee responded favourably to this request, on the grounds that certain items submitted to the proceedings were protected by business secrecy, as provided for in Article L 151-1 of the French Commercial Code.
21. On 10 March 2020, the company's counsel sent CNIL's chairman a request to challenge the rapporteur appointed pursuant to Article 39 of Decree no. 2019-536 of 29 May 2019, on the grounds that he would be biased against the company and its representatives.
22. In a letter in response dated 20 April 2020, the CNIL chairman rejected the request after having pointed out in particular that the request was unfounded and that the documents communicated did not establish the existence of bias by the rapporteur against the company and its representatives.
23. On 23 March 2020, the company submitted observations in response to the report.
24. In an email dated 24 March 2020 and on the basis of Article 40, paragraph 4, of Decree no. 2019-536 of 29 May 2019, the rapporteur asked the chairman of the restricted committee for an additional period of fifteen days to respond to the company's observations.

25. In a letter dated 25 March 2020, taking note of the context of the health crisis, the chairman of the restricted committee granted this request.
26. In a letter dated the same day, the company was informed of the additional period granted to the rapporteur and the fact that it had, pursuant to paragraph 5 of article 40 of decree no. 2019-536 of 29 May 2019, a period of one month to respond to the rapporteur's response. The letter also informed it of the postponement of the restricted committee meeting, initially scheduled for 30 April 2020.
27. On 22 April 2020, the rapporteur notified his response to the company's observations.
28. In a letter dated the same day, CNIL's general secretary informed the company that it could submit its observations to the rapporteur's response until 24 August 2020 pursuant to Order no. 2020-306 of 25 March 2020 on the extension of the deadlines due during the health emergency period.
29. On 11 August 2020, CNIL services notified the company of a notice to attend the restricted committee meeting on 10 September 2020.
30. On 20 August 2020, the company submitted further observations in response to those of the rapporteur.
31. The company and the rapporteur presented oral observations at the restricted committee meeting.

II- Reasons for the final decision

32. According to Article 56(1) of the Regulation "*the supervisory authority of the principal place of business or sole establishment of the controller or processor shall be competent to act as lead supervisory authority regarding the cross-border processing operation carried out by that controller or processor, in accordance with the procedure laid down in Article 60*".
33. In this case, the restricted committee firstly stated that [REDACTED] was founded in France in [REDACTED] and that since that date it has had a registered office in Paris.
34. The restricted committee then noted that this head office, which employs approximately 50 employees, is organised into seven divisions, including a marketing division, a sales division, as well as an IT and development division.
35. Lastly, although the company has several franchise stores worldwide as well as around 100 branches, three of which are located in Spain, the restricted committee noted that these different establishments are only distribution points of the company's products.

36. As a result, [REDACTED] is the sole establishment of the company in the European Union and that CNIL is competent to act as the lead supervisory authority concerning the cross-border processing carried out by this company, in accordance with Article 56(1) of the Regulation.
37. In accordance with the cooperation and consistency mechanism provided for in Chapter VII of the GDPR, the supervisory authorities of the following countries declared themselves affected by this procedure: Germany (Rhineland-Palatinate, Lower Saxony, Berlin, Bavaria), Belgium, United Kingdom, Spain and Luxembourg.
38. The draft decision adopted by the restricted committee was sent to these supervisory authorities on 3 December 2020, pursuant to Article 60(4) of the GDPR.
39. The restricted committee notes that on 1st January 2021, none of the supervisory authorities concerned had raised any relevant and reasoned objection to the draft decision submitted to them, so that they are deemed to have approved it, in accordance with Article 60(6) of the GDPR.

A. Failure to comply with the arrangements for the exercise of the rights of persons (Article 12(2) of the GDPR)

40. According to Article 12(2) of the Regulation, "*the controller facilitates the exercise of the rights conferred on the data subject under Articles 15 to 22 of the Regulation*".
41. **Firstly**, it appears from referral no. [REDACTED] that, on 6 November 2018, a prospect of the company attempted to exercise his right to object to the latter by using the email addresses intended to exercise rights, indicated on the "Personal Data Charter" page of the company's website. The defective nature of these addresses was actually noted by the CNIL delegation during the online audit of 29 April 2019. This malfunction was definitively repaired by the company in May 2019, as was noted during the on-site inspection of 27 and 28 May.
42. The rapporteur argued that, in general, the defective nature of these email addresses has hindered the exercise of the rights of persons. In addition, he noted, in particular, that the company has never granted the request for opposition made by the complainant at the origin of referral no. [REDACTED].
43. In defence, the company argued that this malfunction is due to a simple technical error. It also recalled that after having noted that the electronic addresses had been incorrectly transcribed on its site - the addresses mentioned with a first level domain name in ".fr" instead of ".com" - it restored the correct version on 13 November 2018. It pointed out in this respect that it was only in a second step, upon receipt of the online inspection report of 29 April 2019, that it became aware that this first correction was not sufficient. In fact, the "mailto" field of the hyperlink which allows, when clicking on it, to generate an email directly with the address of the pre-filled recipient, continued to generate emails for "personaldata.fr" instead of

"*personaldatas.com*". For this reason, the actual recovery of these addresses did not occur until May 2019.

44. The company indicated that, in any event, before that date the data subjects could always exercise their rights through the other channels made available to them, for example by sending a letter to the registered office or using the online form dedicated to the exercise of rights.
45. The restricted committee acknowledged that the succession of technical errors made by the company makes it possible to explain in part its delay in restoring the email addresses intended to exercise rights, but it pointed out, firstly, that these explanations do not justify the company's negligence in this matter, more than six months having elapsed between the finding of the defective nature of these addresses and their full repair. Furthermore, the restricted committee again noted that the company only corrected these addresses following the intervention of CNIL delegations.
46. The restricted committee then noted that although, for these six months, the data subjects could always exercise their "data protection" rights through other channels, the simple fact of providing people with a channel that proves to be defective necessarily complicated the exercise of these rights, especially if this channel were supposed to be the simplest to use. In this case, in order to be able to exercise their rights and ensure that their request had been sent, the data subjects had to undertake a new procedure using one of the other channels made available to them by the company when they received an error message informing them of the failure to provide their email, due to the defective "mailto" field.
47. As a result, the restricted committee held that the prolonged defect in these email addresses did not facilitate the exercise of the rights of persons.
48. Lastly, the restricted committee noted that at the date of the hearing, the company had not provided any evidence that it had granted the request for opposition made by the plaintiff at the origin of referral no. [REDACTED].
49. **Secondly**, the restricted committee noted that the checks carried out on 27 and 28 May 2019 were, in particular, intended to investigate several complaints from prospects of the company arguing that they were unable to validly exercise their right of access.
50. The declarations made by the company's representatives in the framework of these audits revealed that, in order to promote its business, the latter conducts, each year, between five and six commercial prospecting campaigns by post and that each of these campaigns represents an approximate volume of 9 million envelopes sent. For each of these campaigns, the company prepares specifications to define, over a period of one to two months, the very concrete terms of the upcoming campaign. These specifications are sent to various service providers of the company, including [REDACTED], which provides the file of persons to be prospected.

51. Therefore, since it determines the purpose and means of the prospecting processing by post, [REDACTED] has the capacity of controller for this processing, while [REDACTED], which acts in this respect on behalf of the former, has the capacity of processor, within the meaning of the Regulation.
52. The findings have made it possible to establish that, when a person who has been the subject of one of these commercial prospecting campaigns by post attempts to exercise his right of access to the "store customer service" of [REDACTED], the latter simply informs it that it does not process its personal data and sends them to [REDACTED] as follows: "*we use a mailing company without having access to personal data, we do not have any more information about you. If you wish to have more details about this, you can write to [REDACTED]*".
53. The rapporteur argued that the terms of the right of access procedure described above do not facilitate the exercise of the rights of data subjects contrary to the provisions of Article 12 of the GDPR.
54. In defence, the company first argued that it fully complies with the requirements of section 12 of the Regulation by ensuring the effective implementation of the rights of persons. It has therefore deployed numerous information media to ensure that all data subjects are informed of their rights and can exercise them through the procedures it has implemented, such as the procedure for requesting the deletion of accounts and/or personal data or the "stop pub" service that its customer service did not hesitate to highlight.
55. The company then argued that it is not responsible for managing a prospect's file belonging to its processor, [REDACTED]. It pointed out that it does not have the means to act on this file, it cannot ensure the effectiveness of the rights of persons in the name and on behalf of that company.
56. The restricted committee noted, first of all, that although [REDACTED] uses a processor in the context of its prospecting operations, it is responsible for the processing carried out and, as such, remains accountable for the obligations associated with this status, particularly those related to compliance with the rights of the data subjects.
57. It then pointed out that the access right procedure implemented for prospects by post necessarily forces prospects who have made a request for a right of access to it to initiate a second step with [REDACTED] to exercise their right. Thus, even if the prospect's right of access request is ultimately successful, this two-step process necessarily extends the processing time. This operational choice has a structural effect that can affect a considerable number of people, with [REDACTED] sending on average over forty-five million mail solicitations for [REDACTED] campaigns.
58. Consequently, the restricted committee considered that in view of the constraints that the right of access procedure places on prospective customers who receive solicitations by post, and

independently of the various information media and procedures put forward by the company, the company does not facilitate the exercise of these people's rights.

59. **Thirdly**, the company claimed to have been the subject of only five complaints.
60. The restricted committee recalled, first of all, in general, that any person encountering difficulties in exercising their rights does not refer the matter to the CNIL, so that the number of complainants cannot be fully representative of the number of people affected by a breach.
61. It then noted that while the number of complaints to CNIL concerning the difficulties encountered in exercising rights with the company is low, the findings made have demonstrated that the actions denounced by the complainants were structural, both as regards the defective nature of the email addresses intended for the exercise of the rights of persons and the excessive complexity of the right of access procedure reserved for prospects receiving solicitations by post.
62. Therefore, and although the company indicated, during the meeting, that it had satisfied 11,633 requests to exercise its customers' rights, the number of persons concerned by the breach of Article 12 of the Regulation, i.e. potentially all of the company's customers, given the systemic nature of the malfunctions, far exceeds the number of complainants who reported this negligence to CNIL.
63. In view of all these facts, the restricted committee considered that the company breached the obligation laid down in Article 12(2) of the Regulation to facilitate the exercise of the rights conferred on the data subjects.

B. Breach of the obligation to ensure the security of personal data (Article 32 of the GDPR)

1. Vulnerability behind the personal data breach suffered by the company

a. *Characterisation of the breach*

64. According to Article 32(1) of the Regulation, "*the controller shall implement appropriate technical and organisational measures to ensure a level of safety appropriate to the risk*".
65. Furthermore, d) of the same paragraph 1 provides that "*as appropriate*", i.e. depending on in particular "*the scope, of the context and purposes of the processing and of the risks*" for the data subjects, the controller shall implement "*a procedure to test, analyse and evaluate the effectiveness of the technical and organisational measures taken to ensure the security of the processing*".

The rapporteur argued that the vulnerability resulting from the breach of personal data suffered by the company resulted in particular from a lack of vigilance by the controller regarding the measures implemented by its data processor responsible for securing its website.

66. In defence, the company first argued that the security obligation resulting from Article 32 of the Regulation is an obligation to provide the means and not to produce a result, so that the finding of a personal data breach does not necessarily involve a breach of this article. It also argued that the rapporteur did not take into account the security measures implemented prior to this breach, which consisted of strengthening the security measures applied to the processing, such as the implementation of two separate servers for the operation of the site or the securing of the entry doors to the servers, as well as strengthening the control of the measures implemented by its processor, in particular through regular exchanges between the company's data protection officer and the latter.
67. The restricted committee recalled that the IT attack leading to the compromise of the personal data of the company's customers was made possible by the exploitation of a vulnerability affecting a module implemented on the company's website, the version of which was obsolete at the time of the attack.
68. First of all, it noted that as of 13 October 2018, it had been posted on the GitHub platform used to make the jQuery-File-Upload module available at the origin of the breach, an update of this module incorporating a patch whose timely installation on the company's website would have made the attack impossible. It further noted that, due to the criticality of this obsolete version of the module, the National Information Systems Security Agency (hereinafter the "ANSSI") had also communicated on this vulnerability and referred to the patch of the module in a publication on its website on 19 October 2018. Thus, on 27 December 2018, the date of the attack on the company's server, the update of the jQuery-File-Upload module incorporating the patch that would have made this attack impossible was put online for more than two months on the GitHub platform and had been relayed by the ANSSI.
69. In this case, the restricted committee pointed out that although the responsibility for the failure to update in due time lies with [REDACTED], which was responsible for securing the company's website, the controller failed to determine the nature of the measures incumbent on its processor, as well as the monitoring of their proper performance by the latter.
70. In this respect, the restricted committee pointed out that it appears from a combined reading of Article 32(1) (d) and Article 28(3) of the Regulation that controllers are required to continue to monitor regularly the effectiveness of the technical and organisational measures implemented to ensure the security of the processing, including the effectiveness of the measures taken by their processor. If, as the company argues, this security obligation is indeed an obligation to provide the means and not to produce a result, it is required throughout the subcontracting relationship and not only at the time of the choice of the latter and the contractualisation of the service.

71. The restricted committee noted that the monthly security reports by which [REDACTED] reports to [REDACTED] on the technical and organisational measures implemented to ensure the security of the website were far from complying with latest industry standards since they did not specify, in particular, whether [REDACTED] regularly carries out a security watch on the site, including the identification and maintenance of its various software components.
72. The restricted committee pointed out, in this respect, that in order to remove this unknown and to draw up a more general assessment of the practices of its processor in terms of IT security, [REDACTED] could have carried out checks or audits of [REDACTED], which the company in question has not proven, despite the fact that the two companies have been in a business relationship since 2013.
73. The restricted committee noted that the responsibility for such shortcomings is all the more attributable to a data controller such as [REDACTED], which, by its scale, had all the material and financial resources sufficient to ensure the security of the data it processes.
74. Consequently, the restricted committee considered that [REDACTED] did not exercise a satisfactory and regular audit of the technical and organisational measures implemented by [REDACTED] to ensure the security of the personal data processed.
75. Moreover, the restricted committee recalled that following a first breach of personal data, [REDACTED] has already been penalised by SAN decision no. 2015-379 of 5 November 2015, certainly concerning different facts, but by which it was sanctioned for not ensuring the security of the personal data for which it was responsible and for not having guaranteed the security of the personal data managed by one of its former processors. Furthermore, following a new breach of personal data that affected its website, the company was again sanctioned by a decision no. SAN-2018-002 of 7 May 2018 for a breach of the security of personal data. After appeal against these decisions, the Council of State confirmed the materiality of these breaches (EC, 19 June 2017, appeal no. 396050 and 17 March 2019, appeal no. 422575)
76. In this respect, the restricted committee noted that [REDACTED] was involved in the facts causing several of the breaches sanctioned in these decisions, so that [REDACTED] should have, in light of these precedents, been particularly alerted as to the defective nature of the guarantees presented by its processor in terms of IT security and, therefore, should have been particularly vigilant.
77. Consequently, the restricted committee held that in light of these previous decisions, [REDACTED] could not be unaware of the importance to be given to IT security issues.

b. Scope of the breach

78. The company argues that the breach did not cause any harm to the customers concerned by the personal data breach, since none of these persons notified them of the fraudulent use of their personal data.

79. The restricted committee noted that it is apparent from the notification sent to CNIL on 11 January 2019 that the personal data breach compromised the personal data of nearly 200,000 European nationals: 189,707 French, 3,326 Belgians, 1,149 Germans, 786 Spanish and 332 British.
80. UK nationals are included as a whole when the United Kingdom was a member of the European Union at the time of the events in question, therefore the GDPR is applicable. Furthermore, under the Trade and Cooperation Agreement concluded on December 24, 2020 between the European Union and the United Kingdom, it appears that despite the United Kingdom's exit from the European Union on January 1, 2021, the GDPR will continue to apply on a transitional basis in the United Kingdom for a maximum additional period of six months from that date.
81. The restricted committee also recalled that the email address, the hash of the user account password, the surname and first names were compromised, address, telephone number, date of birth of customers and, for 23,000 of them, the social security number.
82. It pointed out in this respect that, in view of the nature of these personal data, and in particular the email address/hash pair of the password, the persons affected by the breach are exposed to the risk of reuse of their personal data by attackers, in particular to carry out targeted phishing campaigns or identity usurpations.
83. The restricted committee therefore considers that the company breached the provisions of Article 32 of the Regulation.

2. Lack of security for user account access passwords

84. According to Article 32(1) of the Regulation, "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including among others, as required: (...) B) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.*"
85. The controller must therefore, in accordance with Article 32(2) of the GDPR, take into account the risks posed by the processing, resulting in particular from the destruction, loss, alteration, unauthorised disclosure of personal data transmitted, stored or otherwise processed, or the unauthorised access to such data, accidentally or unlawfully.
86. The CNIL delegation noted, during the online check-up of 29 April 2019, that when creating a user account on the company's website, individuals can use a password of at least eight characters and consisting of only capital letters and figures. In its letter dated 17 September 2019, the company stated that in addition to authentication by login and password, a restriction of access to the account was also implemented, with user accounts being blocked after ten unsuccessful login attempts.

87. The rapporteur argued that the passwords accepted by the company do not ensure the security of the personal data processed in that they are not sufficiently robust and thus do not prevent "brute force" attacks, which consist in the systematic testing of many passwords and which could lead to a compromise of the associated accounts and the personal data they contain.
88. In defence, the company recalled that the rules for creating its passwords had however been redefined in mid-2018. It is surprised by the rapporteur's additional requirements in this regard, noting that for authentication to user accounts of online banks, passwords of a minimum length of five characters are allowed.
89. In its latest submissions, however, it stated that it has reinforced its password policy by requiring that its customers' passwords also contain a special character, but it does not specify whether this reinforcement has also been passed on to customers already having a user account.
90. The restricted committee considers that the length and complexity of a password remain basic criteria for assessing its strength. It noted in this respect that the need for a strong password is also highlighted by ANSSI, which states that "*a good password is above all a strong password, which is difficult to find even using automated tools. The strength of a password depends on its length and the number of possibilities available for each character. In fact, a password consisting of lower cases, capital letters, special characters and numbers is technically more difficult to discover than a password consisting solely of lower cases*".
91. For the sake of clarity, the restricted committee recalled that in order to ensure a sufficient level of security and satisfy the requirements for robustness of passwords, when authentication relies solely on an identifier and password, the CNIL recommends, in its deliberations no. 2017-012 of 19 January 2017, that the password has at least 12 characters - containing at least one capital letter, a lower-case letter, a digit and a special character - or at least eight characters - containing three of these four characters - if it is accompanied by an additional measure such as, for example, the timing of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), setting up a mechanism to guard against automated and intensive attempts (e.g.: "Captcha") and/or blocking the account after several unsuccessful authentication attempts.
92. In this case, the restricted committee considers, first of all, that in light of the weak rules governing their composition, the robustness of the passwords accepted by the society was weak, which put them more at the risk of a brute force attack perpetrated by a hacker.

It then pointed out that this weakness is all the more reprehensible since the user accounts to which these passwords give access contain much personal data concerning the company's customers (email address, surname and first names, postal address, telephone number, date of birth). Some user accounts even contain data of a highly personal nature, such as the social security number, or even within the category of "*special*" data within the meaning of Article 9 of the GDPR, such as medical prescriptions uploaded by customers.

93. Lastly, while online banks can simply offer their customers passwords of a minimum length of five characters, it is because, in addition to the password, authentication to these online accounts also includes additional information, secret, imposed on the user, communicated on its own and with a size of at least seven characters, which most often takes the form of a service ID (customer number or other). Furthermore, for this type of authentication, the requirements for access restrictions are also reinforced (for example, blocking the account after five unsuccessful attempts).
94. Consequently, the restricted committee considers that the passwords put in place by the company to access the user accounts of its website were not sufficiently robust at the time of the findings made by the auditing delegation and that the elements put forward by the company in its last entries do not establish whether the strengthening of its passwords applies to all customers with a user account. Therefore, the company's requirements for the robustness of passwords do not ensure the security of the personal data processed and prevent unauthorised third parties from having access to such data, in breach of Article 32 of the GDPR.
95. In light of all of these elements, the restricted committee considers that the company breached the obligation set out in Article 32 of the Regulation to ensure the security of the personal data it processes.

III. Corrective measures

96. Under the terms of Article 20 III of the law of 6 January 1978 amended:

"When the controller or his processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chair of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order to comply, provided for in II, contact the restricted committee of the authority with a view to the announcement, after adversarial procedure, of one or more of the following measures: [...]

2. An injunction to bring the processing into compliance with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law or to comply with the requests made by the data subject to exercise his/her rights, which may be accompanied, except in cases where the processing is implemented by the State, with a penalty not exceeding €100,000 per day of delay from the date fixed by the restricted committee; [...]

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the restricted committee shall take into account the criteria specified in the same Article 83."

97. Article 83 of the GDPR stipulates that:

"1. Each supervisory authority shall ensure that the administrative fines imposed under this Article for infringements of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive.

2. Depending on the specific characteristics of each case, administrative fines shall be imposed in addition to or instead of the measures referred to in Article 58(2)(a) to (h) and (j). In deciding whether to impose an administrative fine and to decide on the amount of the administrative fine, the following shall be taken into account in each case:

- a) the nature, seriousness and duration of the breach, taking into account the nature, scope or purpose of the processing concerned, the number of data subjects affected and the level of damage they have suffered;*
- b) whether the breach was committed deliberately or due to negligence;*
- c) any action taken by the controller or processor to mitigate the damage suffered by the data subjects;*
- d) the degree of responsibility of the controller or processor, taking into account the technical and organisational measures they have implemented pursuant to Articles 25 and 32;*
- e) any relevant breach previously committed by the controller or processor;*
- f) the degree of cooperation established with the supervisory authority to remedy the breach and mitigate any adverse effects;*
- g) the categories of personal data concerned by the breach;*
- h) how the supervisory authority has become aware of the breach, in particular whether, and to what extent, the controller or processor has notified the breach;*
- i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned for the same purpose, compliance with those measures;*
- j) the application of codes of conduct approved under section 40 or certification mechanisms approved pursuant to section 42; and*
- k) any other aggravating or mitigating circumstances applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the breach."*

98. **Firstly**, concerning the imposition of an administrative fine, the company argued that the CNIL chair should first have sent it an order to comply instead of directly contacting the restricted committee.
99. It added that the amount of any fine imposed should be reduced in view of its cooperation with CNIL's services since the notification of the breach, the non-intentional nature of the breaches alleged against it and the absence of any profits or benefits derived from them.
100. The restricted committee recalled, first of all, that in accordance with Article 20 of the French Data Protection Act, the chair of the CNIL is not required to send an order to comply to the organisation before initiating sanction proceedings against it.
101. Furthermore, if it is established that the company has taken steps to quickly end the personal data breach since the vulnerability was discovered, that it has actively cooperated with CNIL's

services since the notification of the personal data breach and that it has not intentionally committed the breaches of which it is accused, the restricted committee pointed out that the imposition of an administrative fine is no less justified in accordance with the relevant criteria laid down in Article 83(2) of the Regulation.

102. Firstly, the restricted committee recalled that the company has breached two basic IT security obligations, concerning the timely installation of the published critical updates relating to the software it uses and concerning the regular evaluation of the measures taken to ensure the security of the personal data processed, and in particular monitoring of the effectiveness of the technical and organisational measures implemented by its processor.
103. Secondly, it pointed out that the number of persons affected is significant, with the breach of personal data compromising the personal data of nearly 200,000 European nationals. Furthermore, with regard to the procedure for exercising rights, the systemic nature of the malfunctions causing the breach associated with the significant volume of solicitations sent by the company for commercial prospecting purposes, implies that at least hundreds of thousands of prospects or customers of the company are or have been likely to be affected by the two-stage right of access procedure implemented by the company and the defective email addresses indicated for the exercise of rights.
104. Thirdly, it noted that the categories of data exposed by the breach are numerous and reveal personal information, some highly personal, of the lives of individuals, such as their email address, surname and first names, address, telephone number, date of birth and, for 23,000 of them, their social security number. These personal data are also likely to be reused by attackers to carry out phishing campaigns with the data subjects.
105. Lastly, over the past five years, the restricted committee has already twice penalised the company for breaches of personal data security as well as for a breach of subcontracting in the context of previous data breaches.
106. Therefore, since the breaches of Articles 12(2) and 32 of the Regulation are characterised, the restricted committee considers that an administrative fine should be imposed.
107. With regard to the amount of the administrative fine, the restricted committee noted that in 2017 the company achieved a turnover of [REDACTED] and made a profit of [REDACTED] and that pursuant to the provisions of Article 83(5) of the GDPR, it incurs a financial penalty of a maximum amount of €20 million.
108. Therefore, in light of the company's financial capacity and the relevant criteria of Article 83(2) of the Regulation referred to above, the restricted committee considers that imposing a fine of €250,000, which would therefore only represent [REDACTED] of that turnover, appears to be both effective, proportionate and dissuasive, in accordance with the requirements of Article 83(1) of that Regulation.

109. **Secondly**, with regard to the need to issue an injunction, the restricted committee noted that, with regard to the breach of the exercise of rights, the company has not provided any information since the start of the proceedings which would allow it to be considered that it now facilitates requests for access from persons who have been subject to commercial prospecting by post and that it has followed up on the request for opposition from the applicant at the origin of referral no. [REDACTED].
110. Furthermore, with regard to the breach of the security of personal data, the company did not provide any evidence that the strengthening of its password policy was passed on to all its customers, particularly to customers already having a user account.
111. Consequently, if the company fails to comply with the breaches of Article 12(2) and Article 32 of the Regulation, the restricted committee considers that an injunction should be issued.
112. It follows from all of the above and from taking into account the criteria laid down in Article 83 of the GDPR that an administrative fine of €250,000 and an injunction with a penalty are justified and proportionate.

FOR THESE REASONS

The CNIL's restricted committee, after having deliberated, decides to:

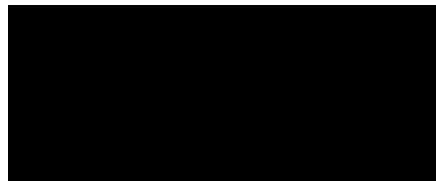
- for breaches of Articles 12 and 32 of Regulation no. 2016/679 of 27 April 2016 on the protection of personal data, order [REDACTED] to pay an administrative fine of €250,000 (two hundred and fifty thousand euros);
- rule against [REDACTED] an injunction to bring the processing into compliance with the obligations resulting from Articles 12 and 32 of Regulation no. 2016/679 of 27 April 2016 on the protection of personal data, and in particular:
 - with regard to the failure to exercise the rights of persons, facilitate all requests addressed to it, in accordance with the provisions of Article 12(2) GDPR, and in particular:
 - facilitate requests for access rights from persons subject to commercial prospecting by post, for example by implementing a mechanism to redirect these requests to its processor effectively and to ensure their follow-up and proper consideration by the processor;
 - provide an exhaustive response to the applicant's request for a right of opposition at the origin of referral no. 19000723;
 - with regard to the breach of the obligation to ensure the security of personal data, take all measures to preserve the security of such data and prevent unauthorised third parties from accessing them pursuant to Article 32 of the GDPR, and in particular:
 - implement a robust and binding password management policy for all user accounts, for example, under one of the following methods:

- passwords shall consist of at least 12 characters, containing at least one letter, a lower case, one digit and a special character;
 - passwords are composed of at least eight characters, containing three of the four character categories (upper case letters, lower case letters, digits and special characters) and are accompanied by a complementary measure such as the timing of access to the account after several failures (temporary access suspension whose duration increases as attempts are made), the establishment of a mechanism to guard against automated and intensive submission of attempts (for example: "captcha") and/or blocking the account after several unsuccessful authentication attempts (maximum ten).
- attach to the injunction a penalty payment of €500 (five hundred euros) per day of delay at the end of a period of three months following notification of this decision, with proof of compliance to be sent to the restricted committee within this period.

The Chairman

Alexandre LINDEN

The Chair



Paris, 06 JAN. 2021

Our ref.: MLD/PVT/SGE/RAL201023

Case submission nos 20006815, 20010739 and 20011014

(please quote in all correspondence)

Dear Madam,

I am writing further to the exchanges between your Data Protection Officer (DPO) and the CNIL, in the context of examining three complaints that were forwarded to us by the Irish Data Protection Commission pursuant to Article 56.1 of the General Data Protection Regulation (GDPR).

These complaints concern [REDACTED] sending of an email to its customers without their email addresses being placed in blind carbon copy (BCC). In an email dated 18 September of this year, your DPO explained that "*the number of email addresses concerned amounted to 37, some of which were generic email addresses associated with legal entities*".

Moreover, it has been specified that this incident is due to a human error committed by your service provider [REDACTED] in the context of using an IT tool for sending "*emails to all of the people of a flight*".

First, I would remind you that, as data controller, it is your responsibility to ensure the security and privacy of the personal data you process, including through your processors, by implementing appropriate technical and organisational measures (Article 32, GDPR).

On that note, provision must be made for measures that are aimed at preventing an email being sent to a group of individuals without the recipients' email addresses being placed in the "BCC" field to ensure they are invisible, including when a processor sends such emails.

Second, I would point out that such actions amount to a personal data breach under Article 4.12 of the GDPR, but that no personal data breach has been notified to the CNIL in this regard.

Now, the provisions of Article 33 of the GDPR provide that "*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*".

RÉPUBLIQUE FRANÇAISE

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

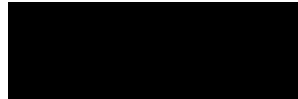
Although your DPO has explained that, in light of the low volume of personal data concerned by said breach, [REDACTED] did not consider it necessary to communicate the breach to the data subjects as stipulated in Article 34 of the GDPR, the breach in question does seem likely to generate a risk – even a moderate one – for the data subjects. As such, [REDACTED] failed to comply with its obligation to notify such a breach to the CNIL.

I note that, since this incident, "*a reminder of the procedure*" has been issued to "*all of [your] service provider's staff*" to ensure it does not happen again. However, all of these facts prompt me, in agreement with the other European data protection authorities concerned by the processing, to remind [REDACTED] of its obligations regarding the aforementioned points, in accordance with the provisions of Article 58.2.b) of the General Data Protection Regulation (GDPR).

The requirements reiterated above must be fulfilled without fail in the future. Where necessary, the CNIL will conduct subsequent verifications and reserves the right to apply the whole panoply of powers conferred upon it by the GDPR and the French Data Protection Act (Act of 6 January 1978 amended).

My staff ([REDACTED] [@cnil.fr\) is at your disposal for any further information.](mailto:@cnil.fr)

Yours sincerely,



This decision may be appealed before the French Conseil d'Etat within two months of its notification.

NB: Copy to [REDACTED] Data Protection Officer at [REDACTED]

Summary Final Decision Art 60

Complaint

Reprimand

EDPBI:FR:OSS:D:2021:169

Background information

Date of final decision:	6 January 2021
Date of broadcast:	6 January 2021
LSA:	FR
CSAs:	IE
Legal Reference:	Notification of a personal data breach to the supervisory authority (Article 33), Communication of a personal data breach to the data subject (Article 34)
Decision:	Reprimand
Key words:	Electronic communications, Personal data breach

Summary of the Decision

Origin of the case

The Controller send an email to its customers with their email addresses being visible for all recipients (the controller did not place the email addresses in bcc). The number of email addresses amounted to 37. The LSA received three complaints concerning that incident.

Findings

The LSA found that the incident is due to a human error committed by the controller's service provider. The LSA stated that the incident constitutes a personal data breach under Article 4.12 GDPR. The LSA found that the breach in question did seem likely to generate a risk for the data subjects and considered that the controller failed to comply with its obligation to notify a breach to the supervisory authority according to Article 33 GDPR.

The controller took steps to prevent such incident in the future, namely issued a reminder to all of controller's service provider's staff regarding the procedure on sending emails.

Decision

The LSA issued a reprimand regarding controller's obligations pursuant to Article 33 GDPR in accordance with the provisions of Article 58.2.b) GDPR.

Summary Final Decision Art 60

Legal obligation, complaint

Administrative fine

EDPBI:FR:OSS:D:2021:181

Background information

Date of final decision:	06 January 2021
Date of broadcast:	12 February 2021
LSA:	FR
CSAs:	BE, DE-BE, DE-BY, DE-NI, DE-RP, ES, LU, UK
Legal Reference(s):	Transparency and Information (Article 12), Security of processing (Article 32)
Decision:	Compliance order, Administrative Fine
Key words:	Personal data breach, Data security, Password, Data subject rights

Summary of the Decision

Origin of the case

Following the notification of a personal data breach (intrusion attack on the controller's website affecting 210,692 European nationals), the LSA conducted both an on-site and online audits of the controller in order to verify its compliance with the GDPR, in particular with regard to the aforementioned data breach.

Thereafter, the LSA carried out a second on-site control of the controller in the context of the LSA's investigations regarding five complaints received from customers and prospects concerning the commercial prospecting by the controller they have been subject to, as well as the exercise of their rights.

Findings

The LSA found that the controller did not facilitate the exercise of data subject rights as the email address provided to them for this purpose was defective. In addition, the LSA pointed out the complexity of the right of access procedure implemented by the controller for prospects receiving

postal solicitations. Therefore, the LSA considered that the controller failed to comply with its obligations under Article 12(2) GDPR.

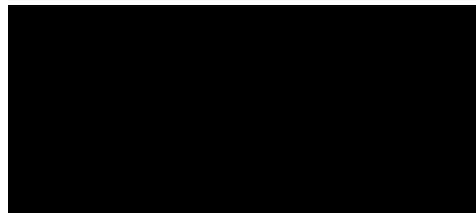
As a result of its investigations regarding the data breach notification, the LSA found that the controller had failed to ensure the security of the personal data it processed (Article 32 GDPR). Firstly, the LSA found that the controller did not ensure the effectiveness of the technical and organisational measures implemented by its processor. In this regard, the LSA concluded that the controller should have been more vigilant in complying with security standards considering that it had already been sanctioned by the LSA for security issues involving this same processor. Finally, the LSA considered that the controller's requirements regarding the robustness of passwords were insufficient to ensure the security of the personal data processed and to prevent third parties from accessing the personal data.

Decision

The LSA imposed an administrative fine of 250,000 euros to the controller.

In addition, the LSA imposed a compliance order on the controller to remedy its breaches of Articles 12 and 32 GDPR with a penalty payment of 500 euros per day of delay at the end of a period of 3 months following the notification of the decision.

The President



Registered letter with AR

N°:

Paris, the 31 MARS 2021

Our Ref.: MLD/CHT/RAL201030

Case n°19016963

(to be referenced in all correspondence)

Dear M. President,

I am writing further to the complaint of [REDACTED], transmitted to the CNIL by the Spanish Data Protection Authority ("Agencia Española de Protección de Datos") pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] filed a complaint with her national data protection authority against [REDACTED] which belongs to the [REDACTED] and is domiciled in France, regarding a personal data breach committed during an order on the [REDACTED] website on 6 November 2018. This breach results from a fraudulent intrusion on the [REDACTED] e-commerce platform installed on this website between 0:11 am on 3 November 2018 and 12:52 pm on 8 November 2018.

The exchanges that have taken place between the CNIL departments and the [REDACTED] DPO Office in connection with the investigation of this complaint lead me, in agreement with the other European data protection authorities concerned by this personal data breach, to remind [REDACTED] of its obligations regarding the following points, in accordance with the provisions of Article 58.2.b) of the GDPR.

In the event of a personal data breach, [REDACTED] is required to notify the relevant **supervisory authority** of the breach in question as soon as possible and, if possible, 72 hours after becoming aware thereof, unless the breach in question is unlikely to result in a risk to the rights and freedoms of individuals.

RÉPUBLIQUE FRANÇAISE

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

In this case, the UK and Dutch supervisory authorities were notified of the breach on 16 November 2018. Your services have indicated to the Commission that this choice of notifications lies in the fact that, on the one hand, the Netherlands is where [REDACTED] registered office is located and is designated in the general terms of use of the website as the place of jurisdiction and that, on the other, England is this website's main country of operation.

However, your data protection officer has also confirmed to us that [REDACTED] is the data controller implicated in this case.

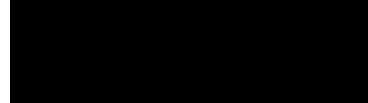
Therefore, the notification should have been made to the French data protection authority, the CNIL, pursuant to Article 33.1 of the GDPR.

I also note the measures taken to avoid the repetition of such events.

[REDACTED] in fact proves that the individuals concerned were notified by an email from [REDACTED] sent on 16 November 2018 to each of the individuals identified as victims of the breach, as well as by a message on its website. Similarly, your services report security audits conducted on the [REDACTED] platform and a set of measures taken regarding its architecture, as well as PCI SAQ 3.2 rev. 1.1 certification.

Finally, I would like to point out that this decision, which closes the examination of [REDACTED] complaint, does not preclude the CNIL from using, in the event of new complaints, all the other powers conferred to it under the law of January 6th, 1978 as amended and the GDPR.

Yours sincerely,



Marie-Laure DENIS

Copy to [REDACTED] Data Protection Officer

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

**Decision no.MED 2021-013 of 1st April 2021 issuing an order to comply to
the company [REDACTED]**

(No. MDM211014)

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

Having regard to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of personal data and the free movement of such data, its Articles 56 and 60 in particular;

Having regard to Act no.78-17 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act), its Article 20 in particular;

Having regard to Decree no.2019-536 of 29 May 2019, implementing Act no.78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to Deliberation no.2013-175 of 4 July 2013 adopting the Internal Rules of Procedure of the *Commission Nationale de l'Informatique et des Libertés*;

Having regard to decision no.2019-13C of 27 December 2019 of the Chair of the *Commission Nationale de l'Informatique et des Libertés*, tasking the Secretary-General with performing or assigning a third party to conduct an investigation of the [REDACTED] company;

Having regard to Online Investigation Record no.2020-013/1 of 15 January 2020;

Having regard to Onsite Investigation Record no.2020-013/2 du 23 January 2020;

Having regard to Referral no.19018488;

Having regard to the other items in the case file.

I. Context

The [REDACTED] (hereinafter, the “Company”), better known under its former trade name [REDACTED], runs a platform for rental of vehicles (cars and motorbikes) which puts vehicle owners in contact with private individuals. It employs about 133 people at its head office, located at [REDACTED]. Its turnover in 2018 was [REDACTED] euros.

In the context of its activity, the Company publishes [REDACTED] website and the [REDACTED] mobile application, which target consumers living in France and other European Union countries.

The platform provides two ways of renting vehicles:

- using the [REDACTED] technology, which enables the customer to unlock the hired car using a smartphone (via a unit installed in the vehicle) without meeting the owner. Identity documents and driving licenses, which are required for rentals, are checked directly by the application, as are driver records. If the check of supporting documents fails (due to poor quality document or suspicion of fraud), the user can have them checked manually by sending an email to the Company’s customer service. The

- email is automatically turned into a ticket by the [REDACTED] company, a subcontractor specialising in management of customer relations, utilised by [REDACTED];
- without [REDACTED]: in this case, users have to make physical contact with car owners, who check the supporting documents and hand them the car keys in person.

On 15 October 2019, a complaint was referred to the *Commission nationale de l'informatique et des libertés* (hereinafter, the “CNIL” or the “Commission”) from one of the Company’s customers, who reported that his driving license was accessible via any browser with no authentication required, by entering an URL that connected to the [REDACTED] software tool. The complainant also stated that despite his making several requests for deletion to the Company’s services, his driving license was still freely accessible on the date of the referral.

Pursuant to The Chair of the Commission’s Decision no.2020-13C of 27 December 2019, a CNIL Delegation conducted an online investigation of the Company’s website on 15 January 2020 and an onsite investigation at the Company’s premises on 23 January 2020, in order to check whether the personal data processing operations it implemented were in compliance with Regulation no.2016/679 of the European Parliament and the Council of 27 April 2016 on personal data protection (hereinafter, the “GDPR”).

In a mail sent on 14 February 2020 subsequent to the onsite control, the Company stated that it “*had been able to get the [REDACTED] tool’s configuration modified so that any documents sent by [its] users via email would no longer generate the URL link. Users who send documents by email now receive a confirmation email with the said document as a simple attachment*”.

On 27 May 2020, following the Company’s communication of documents requested in the context of the onsite investigation, the CNIL’s departments conducted a complementary investigation on the documents, in the context of which the Company was requested to complete a questionnaire before 1 July 2020.

On 3 July 2020, the Company sent the CNIL’s departments the completed questionnaire.

On 3 September 2020, in the context of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

II. Breaches of the GDPR’s provisions

A. A breach of the obligation to define and comply with a retention period proportionate to the purposes of the processing

Pursuant to Article 5, Paragraph 1, e) of the GDPR, “*personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*”.

In this instance, although the onsite investigation showed that the Company had defined a policy on data retention periods in a document entitled “*Privacy deletion policies*”, the Company’s representative nonetheless told the Delegation that, in practice, there had been no restrictions on retention periods for users’ data relating to creation of their accounts on the [REDACTED] platform since the Company’s creation.

In its letter of 3 July 2020, the Company stated that its database contained the accounts of 874,000 users whose last connection had been in 2016 but that it was able to specify the number of users who had connected for the last time before 2016.

Finally, the Company's representatives stated that there was no intermediate archiving of data.

The aforementioned facts constitute a breach of the obligations of Article 5, Paragraph 1, e) of the GDPR. It is therefore the company's responsibility to define and enforce retention periods for user data.

B. A breach of the obligation to comply with requests for erasure of data

Under Article 17, Paragraph 1, a) 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 the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed*".

In this instance, the case file shows that, since 30 August 2019, the complainant at the origin of Referral no. 19018488 has requested the Company on several occasions to erase his driving license, which had been made freely accessible via a link automatically generated by the [REDACTED] software tool.

During the onsite investigation conducted on 23 January 2020, the Delegation found that the Company had not erased the driving license, which was still accessible via the aforementioned link.

Although, in its letter of 14 February 2020, the Company stated that any documents that users sent by email would no longer generate a URL link, in its response of 3 July 2020 to the questionnaire sent by the Delegation it nonetheless wrote that it was "*unable to delete the links that had previously been created and that these therefore still exist*".

This most recent statement makes it clear that the Company has not yet erased the complainant's driving license.

Moreover, during the onsite investigation and in their letter of 14 February 2020, the Company's representatives stated that when it receives a request for erasure, the Company "*anonymises*" the data subject's customer record in the customer management tool. However, the Investigation Delegation found that, despite such "*anonymisation*", the user's number was still in the database.

In its Opinion 05/2014 of 10 April 2014, which provides useful hints on assessment of a piece of data's identifiable character, the Article 29 Working Party (WP29) defined anonymisation as the result of "*processing personal data in order to irreversibly prevent identification*".

In this case, customer records created by the Company are not anonymised within the meaning of the GDPR, as it is still technically possible to re-identify customers from their

user numbers. For example, an attacker who managed to unlawfully infiltrate the Company's servers would be able to take note of these numbers, which are also stored unencrypted, and cross-reference them with other indirectly identifying personal data in their possession in order to try to discover the identities of the individuals behind such data.

It follows that the general data erasure procedure implemented by the Company does not guarantee data subjects' right to erasure.

The aforementioned facts constitute a breach of the obligations resulting from Article 17 of the GDPR. It is the company's responsibility to comply with requests for the deletion of personal data that are made to it.

C. A breach of the obligations relating to data processors

Under Article 28, Paragraph 3 of the GDPR, all processing implemented by a data processor must be governed by a contract, concluded between the data controller and the processor which binds both parties, "*sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller*". Hence, the contract must include a series of mandatory terms, as detailed in points a) to f) of the same Article.

In this instance, during the onsite investigation, the Delegation was informed that the Company had entrusted verification of the identities of its users' profiles to two service providers, [REDACTED] and [REDACTED].

[REDACTED] has developed a robot responsible for validating the various supporting documents provided by users (driving license, identity document and video selfies). When the robot does not validate a profile (e.g. because of the poor quality of a photo), the check is carried out manually by a [REDACTED] employee.

It follows that [REDACTED] and [REDACTED] process personal data on behalf of [REDACTED] and therefore act as data processors for the Company.

However, the Inspection Delegation found that the service provision contract concluded with [REDACTED] on 9 July 2019 and the one concluded with [REDACTED] on 25 July 2019 do not specify all the terms provided for by Article 28, Paragraph 3 of the GDPR.

The contract concluded with [REDACTED] does not define the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, or the obligations and rights of the controller. Nor does it specify that the processor undertakes to:

- process the personal data only on documented instructions from the controller (Article 28, 3. a));
- respect the conditions [...] for engaging another processor (article 28, 3. d));
- assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Article 28, 3. f));
- delete or return all the personal data to the controller after the end of the contract (Article 28, 3. g));

- make available to the controller all information necessary to the carrying out of audits (article 28, 3. h)).

Although the contract concluded with [REDACTED] defines the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, it does not include any of the terms listed in Article 28, Paragraph 3 of the GDPR.

The aforementioned facts constitute a breach of the obligations resulting from Article 28 of the GDPR. It is the responsibility of the company to complete the subcontract.

D. A breach of the obligation to keep a record of processing activities

A combined reading of Paragraphs 1 and 5 of Article 30 of the GDPR makes it clear that a data controller with over 250 employees and/or which carries out processing of personal data on a regular basis must maintain a record of processing activities carried out under its responsibility.

Such record must contain the following information:

- the name and contact details of the controller,
- the purposes of the processing,
- a description of the categories of data subjects and of the categories of personal data,
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations,
- the envisaged time limits for erasure of the different categories of data,
- a general description of the technical and organisational security measures referred to in Article 32, Paragraph 1 of the GDPR.

In this case, although the Company has fewer than 250 employees, it carries out a variety of personal data processing operations regarding prospects and customers, for such purposes as marketing, customer management and combating fraud. Insofar as the Company's main activity is based on a platform that puts vehicle renters and owners in contact with each other, there can be no doubt that such processing is carried out on a regular basis.

However, statements made by the Company's representatives make it clear that, on the date of the onsite investigation, the Company did not keep a record of processing activities.

The aforementioned facts constitute a breach of the obligations resulting from Article 30 of the GDPR. It is the company's responsibility to set up this record of processing activities.

E. A breach of the obligation to ensure data security and confidentiality

Under Article 32 of the GDPR, "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [including by guaranteeing] the ongoing confidentiality, integrity, availability and resilience of processing systems and services*".

Firstly, as regards the security measures applied to supporting documents that platform users send by email, in its letter of 14 February 2020, the Company stated that it had requested its

processor to modify the [REDACTED] tool’s configuration so that any documents emailed by users would no longer generate the URL link, and that users who send supporting documents by email now receive a confirmation email with the said documents as attachments.

However, in its letter of 14 February 2020 and in the response on 3 July 2020 to the questionnaire sent by the Delegation, the Company stated that it was “*unable to delete the links that had previously been created [by the [REDACTED] tool] and that these therefore still exist*”. Nonetheless, it asserted that the URL links that had been created could not be the subject of brute force attacks as they contained several lines of characters, that such length could not be retrieved and that it therefore applied a robust rule of “*security through obscurity*”.

Although it is true that the length of the URLs in question makes it unlikely that a brute force attack against them would succeed, the simple fact that the supporting documents they link to are accessible without prior authentication is a risk factor all too likely to compromise the confidentiality of data subjects’ personal data. For example, as the URLs are apparently hosted in [REDACTED] servers’ logs unencrypted, an attacker who unlawfully infiltrated the servers could easily transcribe the web addresses in order to access users’ supporting documents and make use of them for the purpose of identity theft.

Secondly, as regards the security measures applied to storage of platform users’ passwords, the Company stated during the onsite investigation that it had been using the Bcrypt algorithm since 2013 and that this security measure covers 3,083,296 user accounts.

In its letter of 14 February 2020, the Company stated that 164,394 user account passwords created before 2013 are retained in a database in hashed format, using the SHA1 algorithm with salt. It also stated that, since 27 January 2020, users whose passwords are hashed with the SHA1 algorithm have had to use the “*I’ve forgotten my password*” functionality when they want to authenticate themselves on their accounts and so obtain a new password hashed under the Bcrypt +salt standard. Hence, accounts operating with SHA1 passwords have not been usable since 27 January 2020.

The above information makes it clear that, although the Company has ensured that authentication on the platform is now only possible in accounts whose passwords are hashed by the Bcrypt algorithm, it still retains the passwords to over 150,000 user accounts in a form that does not ensure their confidentiality.

The SHA1 hashing function has known vulnerabilities that make it impossible to guarantee integrity and confidentiality of passwords in the event of a brute force attack after the servers hosting them have been compromised. Inasmuch as a great many internauts use the same password to authenticate themselves on their various online accounts, attackers could well exploit these 150,000 users’ passwords to infiltrate their other accounts in order to perpetrate thefts or scams.

Thirdly, as regards the security measures applied in the context of replies to right of access requests, during the onsite investigation the Company’s representatives stated that data to which right of access is requested are communicated to data subjects via two separate emails: one containing a data extract in CSV format, in the form of an encrypted archive, and the other containing the password to the archive.

Although the Company encrypts the archive containing personal data, it sends the password to it by the same channel, so exposing the data communicated to a risk of compromise in the event of an attacker's intrusion into the data subject's inbox or interception of emails by an unauthorised third party.

The aforementioned facts constitute a breach of the obligations resulting from Article 32 of the GDPR. It is the company's responsibility to ensure the security of the personal data it processes.

Consequently, the [REDACTED] company, located at [REDACTED], is issued an order to comply, within three (3) months as from notification of this decision and subject to measures that it may already have adopted, by:

- **defining and implementing a policy on a retention period for its customers' and prospects' data** that does not exceed the period necessary for the purposes for which they are collected, pursuant to Article 5, Paragraph 1, e) of the GDPR, in particular by purging or ensuring effective anonymisation of data retained beyond the period defined, and, for example, by implementing an effective procedure for archiving such data with restricted access;
- **defining and implementing an effective right to erasure procedure**, pursuant to Article 17 of the GDPR, and, in particular, deleting the complainant's supporting documents and erasing or ensuring effective anonymisation of customer records on individuals who have requested that all their personal data be erased;
- **completing the contracts with [REDACTED] and [REDACTED] by including the missing terms**, pursuant to Article 28, Paragraph 3 of the GDPR;
- **keeping a record of processing activities carried out under its responsibility** pursuant to Article 30 of the GDPR;
- **taking all necessary security measures for all personal data processing carried out, so as to ensure the security of such data and prevent unauthorised third parties from accessing them**, pursuant to Article 32 of the GDPR, in particular:
 - by making all supporting documents still retained in the form of links in the [REDACTED] tool inaccessible by third parties without prior authentication, possibly by having them communicated in the form of attachments, as has been done for supporting documents sent following modification of [REDACTED] configuration;
 - by replacing the SHA1 hashing algorithm with salt by an algorithm acknowledged to be strong, for passwords to the [REDACTED] user accounts concerned, possibly by obliging users to c r by deleting their passwords;
 - by using different channels for sending personal data in the form of encrypted archives and the password, possibly by sending the password by SMS when the encrypted archive is sent by email.
- **justifying to the CNIL that it has complied with all of the above requests within the time-limit set.**

After this time-limit has expired, if [REDACTED] has complied with this order, this procedure will be considered closed and a letter to that effect will be sent to it.

However, if [REDACTED] has not complied with this order, a rapporteur will be appointed and may request that the Restricted Committee impose one of the sanctions provided for in Article 20 of the Act of 6 January 1978 amended.

The Chair

Marie-Laure DENIS

The Chairwoman



Paris, - 9 AVR. 2021

Our Ref.: MLD/LCN/RAL211005

Ref. No 20019872

(to be quoted in all correspondence)

Dear Sir,

I am following up on the various exchanges that have taken place between the services of the *Commission Nationale de l'Informatique et des Libertés* (“CNIL” - French Data Protection Authority) and the Digital Protection Officer of [REDACTED] as part of the investigation of [REDACTED] [REDACTED] complaint, transmitted to the CNIL by the Belgian Data Protection Authority (“DPA” - Belgian Data Protection Authority) pursuant to Article 56.1 of the General Data Protection Regulation (“GDPR”).

[REDACTED] had lodged a complaint with his national data protection authority against [REDACTED] concerning difficulties in exercising his right to portability and his right to erasure.

The failures noted at the time of the exchanges between the CNIL and [REDACTED] lead me, in agreement with the other European data protection authorities concerned by the processing implemented, to remind [REDACTED] of its obligations, in accordance with the provisions of article 58.2.b) of the GDPR.

In this case, [REDACTED] exercised his right to the portability and deletion of his data following the termination of his contract with [REDACTED]. These requests have not been answered.

[REDACTED] has acknowledged that it had failed in its obligations by not responding to [REDACTED] requests. It also stated that the data collected from customers, namely the telephone number and IP address, were not “elements giving rise to portability” on the one hand, and confirmed to us that the personal data concerning [REDACTED] had been deleted, on the other hand.

However, I would remind you that Article 20 of the GDPR provides that, when certain conditions are met, “*the data subject shall have the right to receive personal data concerning him or her, which he or she has provided to a controller in a structured, commonly used and machine-readable format*”.

RÉPUBLIQUE FRANÇAISE

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

Therefore, when [REDACTED] receives a request for data portability, it must provide the applicant with the data that he or she has communicated at the time of subscription, as well as the data generated by his or her activity, provided that these are processed in an automated manner and based on prior consent or on the performance of a contract.

Therefore, following his request, you should have transmitted to [REDACTED] all the personal data concerning him provided or generated in the context of the subscription with your services.

In this case, I understand from your reply that the data have been deleted in the meantime and that there is therefore no longer any reason to transmit them. The request for deletion is therefore no longer applicable.

In any case, and in a general way, you must inform the person of the outcome of his or her request within one month of receiving it (Article 12.3 of the GDPR), mentioning that he or she can lodge a complaint with the competent data protection authority and seek legal redress (Article 12.4 of the GDPR).

You will find a great deal of information on this subject on the CNIL website, in particular on the “*Compliance tools*” page, which can be accessed via the following URL <https://www.cnil.fr/fr/les-outils-de-la-conformite>.

Finally, I would like to point out that this decision, which closes the investigation of [REDACTED] [REDACTED] complaint, does not exclude the CNIL from making use, particularly in the event of new complaints, of all the other powers attributed to it by the RGPD and by the amended Act of 6 January 1978.

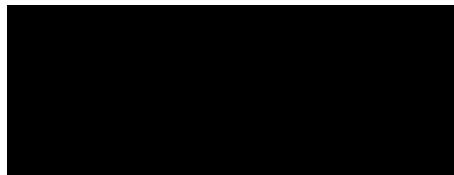
Yours sincerely,



Marie-Laure DENIS

This decision may be appealed to the Council of State within two months of its notification.

The President



Examination of the case:

Paris, le
[REDACTED]

No./Ref.: MLD/DAU/CM211730

Case no. 20013084

(To be referenced in all correspondence)

Sir,

This is further to the exchanges that took place between the services of the French data protection authority (Commission nationale de l'informatique et des libertés « CNIL ») and the lawyer of [REDACTED] within the framework of the examination of [REDACTED] complaint, transmitted to the CNIL by the Norwegian data protection authority (« Datatilsynet ») pursuant to Article 56.1 of the General Data Protection Regulation (« GDPR »).

[REDACTED] had lodged a complaint with his national personal data protection authority against the [REDACTED] concerning the alleged transmission of one of his personal message (whose content is « *We must secure the existence of our people and a future for white children* ») by [REDACTED] to a third party, the [REDACTED].

The latter had requested your services by email dated April 6th, 2020 about the purposes and the legal basis of such transmission, without obtaining any answer.

Our exchanges lead me, in agreement with other European data protection authorities concerned by the processing of data of users of the website [REDACTED] to proceed to the closure of this complaint.

Indeed, first of all, I take note that [REDACTED] is not at the origin of the transmission of the message at stake to the [REDACTED]

In this case, users of [REDACTED] services, recipients of this message, have transmitted it directly to the personal address of the Tournament Director of the [REDACTED], who also turns out to be a volunteer moderator of [REDACTED]. The latter has then transmitted again this message to the competent service of the [REDACTED], in his quality of Director, but not as a moderator, from his personal address. Therefore, tools made available to the moderators by [REDACTED] have not been used, for obtaining, nor for transmitting the private message at stake.

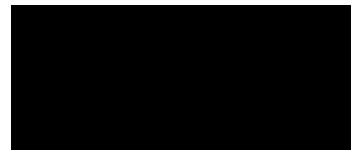
RÉPUBLIQUE FRANÇAISE

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

In any event, I do bring your attention on the necessity for [REDACTED] to implement appropriate technical and organisational measures, in order to ensure that its moderators do not share personal data obtained within their moderation with third parties, in accordance with Article 32 GDPR.

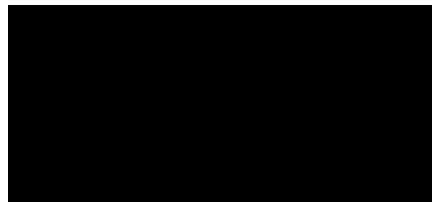
Furthermore, although data protection authorities are not competent to assess the lawfulness of the complainant's account lockout took by [REDACTED] further to the insulting messages pronounced by the latter, [REDACTED] had to inform him about the reasons leading to his exclusion from the service, as well as about the duration of such exclusion, at least when receiving the complainant's request for explanations. Therefore, I do invite you to provide such information to [REDACTED].

Yours Sincerely,



Marie-Laure DENIS

The President



Registered letter with AR

AR No: 2C 157 386 0318 4

Investigation of the case:

Paris, on 09 JUIN 2021

Our Ref.: MLD/CHT/CM21001365

Case n°20016122

(to be referenced in all correspondence)

Dear Sir

I am writing further to the complaint of [REDACTED], transmitted to the Commission nationale de l'informatique et des libertés (CNIL) by the data protection authority in Luxembourg ("the Commission nationale pour la protection des données du Grand-Duché de Luxembourg (CNPD)") pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] lodged a complaint with his national data protection authority against the company [REDACTED], established in France, which had not responded to his request for access to his personal data, including the origin of the data.

The exchanges that have taken place between CNIL services and [REDACTED] Data Protection Officer (DPO) in the context of the investigation of this complaint lead me, in agreement with the other European data protection authorities concerned by prospecting and data management processing of your prospects, **to close this complaint**.

Firstly, with regard to the exercise of the complainant's right of access, I note that [REDACTED] request for right of access, made on 30 March 2020, was taken into account by your services which replied to him on 20 April 2020, i.e. within the one-month time limit provided for in Article 12.3 of the GDPR. I note that this response includes a description of the origin of the personal data concerning him, the legal basis for your data processing and a copy of all personal data concerning the complainant held by [REDACTED].

Although your DPO informed my services that the reply made to [REDACTED] did not include, in the body of the e-mail, all the information indicated in Article 15.1 of the GDPR, she nevertheless indicated that from now on the replies to requests for right of access will include all these elements.

RÉPUBLIQUE FRANÇAISE

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

Secondly, I note that [REDACTED] has been solicited by your services on his professional address within the framework of a recruitment campaign in connection with his professional activity. Concerning the origin of the personal data concerning him, I take note that they were collected through recruitment platforms to which [REDACTED] would have communicated these data; platforms with which you are bound by a commercial contract.

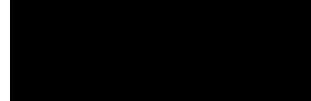
Thirdly, with regard to informing individuals about the identity of the advertiser and the means of objecting to new solicitations, your DPO informed my services that the mail received by [REDACTED] was part of [REDACTED] first information campaigns, in which the identity of the data controller was shown (logo and redirection link to the website where the information was available) and a link was provided to the website to access unsubscribe procedures. Since then, marketing emails include more detailed information on the origin of the data, the purpose of the processing and its legal basis, the contact address of your data protection team, an unsubscribe link and a link back to your data protection policy.

Finally, your DPO has indicated to my services that [REDACTED] did not receive any further requests from [REDACTED] following the reply sent to him on 20 April 2020, and that he was never contacted again by your services for similar campaigns.

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

However, the CNIL reserves the right, in the event of new complaints, to make use of all the powers granted to it by the GDPR and the amended Act of 6 January 1978.

Yours sincerely



Marie-Laure DENIS

Copy to [REDACTED] Data Protection Officer

Final decision of restricted committee No. SAN-2021-008 of 14 June 2021 concerning [REDACTED]

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr. Alexandre LINDEN, Chairman [REDACTED] and [REDACTED]

Having regard to Regulation (EU) 2016/79 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 Post and Electronic Communications Code;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing Act No. 78-17 of 6 January 1978 on data protection;

Having regard to Decision No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL;

Having regard to Decision No. 2018-238C of 27 September 2018 of the CNIL Chair to instruct the secretary general to carry out or have a third party carry out an assignment to conduct verifications of the processing implemented by that organisation or on behalf of [REDACTED]

Having regard to the decision of the CNIL Chair appointing a rapporteur before the Restricted Committee of 19 December 2019;

Having regard to the report of [REDACTED] commissioner rapporteur, notified to [REDACTED] on 2 October 2020;

Having regard to the written observations submitted by [REDACTED] on 2 November 2020;

Having regard to the rapporteur's response to the observations notified on 24 November 2020 to the company's counsel;

Having regard to the written observations of [REDACTED] received on 16 December 2020 and the oral observations made at the restricted committee meeting;

Having regard to the document relating to [REDACTED] ent of the procedure for the intermediate archiving and anonymisation of the data of [REDACTED]'s prospects and customers submitted by the counsel of [REDACTED] at the meeting of the restricted committee;

Having regard to the bailiff's minutes drawn up on 5 February 2021 and its appendix, sent by the company's counsel to the chairman of the restricted committee and to the rapporteur on 10 February 2021;

Having regard to the other documents in the file;

The following were present at the Restricted Committee session on 28 January 2021:

- [REDACTED] Commissioner, heard in her report;

In their capacity as representatives of [REDACTED]

- [...]

[REDACTED] having last spoken;

The restricted committee adopted the following draft decision:

I. Facts and proceedings

1. [REDACTED] (hereinafter “the company”) is a simplified joint stock company with a single shareholder, created in 2012. Its registered office is located at [REDACTED]. It is chaired by [REDACTED] a simplified joint stock company, located at the same address.
2. The company publishes the [REDACTED] website, which has been accessible in France and Spain since 2015, Italy since 2016, and Portugal since 2017. It is a [REDACTED]. [REDACTED] sales were only available if you had created an account on the site. Since then, sales are visible without the need to create an account prior to viewing them. However, to make a purchase, it is still necessary to create an account on the [REDACTED] website. In 2018, the company had [REDACTED] users in France, [REDACTED] users in Spain, [REDACTED] users in Italy, and [REDACTED] users in Portugal.
3. In 2018, the company generated revenue of approximately [REDACTED] euros and a net profit of approximately [REDACTED] euros. In 2019, it generated revenue of [REDACTED] euros and a net profit of approximately [REDACTED] euros. In 2020, the Company generated revenue of approximately [REDACTED] euros and a net profit of approximately [REDACTED] euros. In 2018, [REDACTED] employed approximately 150 persons.
4. On 13 November 2018, pursuant to the CNIL chair’s Decision No. 2018-238C of 27 September 2018, a CNIL delegation carried out an audit at the premises of [REDACTED]. The purpose of this audit was to verify compliance by the company with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter “the Regulation” or “GDPR”) and with the amended Act No. 78-17 of 6 January 1978 on data protection (hereinafter “the amended Act of 6 January 1978” or “the French Data Protection Act”).
5. The audit focused on the processing of personal data of the company’s customers and prospects. The verifications concerned in particular the retention periods for personal data are kept, the information provided to data subjects regarding the processing carried out by the company, compliance with requests for the erasure of personal data from data subjects, the obligation to ensure data security and the obligation to obtain the consent of the data subject to receive marketing messages by e-mail.
6. At the end of the audit, minutes No. 2018-238/1 were notified to the company [REDACTED] by letter dated 19 November 2018. The company sent the CNIL, by e-mail sent that same day, the additional documents requested at the end of the audit.
7. By e-mail of 5 February 2019, the company provided the delegation with several additional documents on its own initiative, including a document entitled “Personal data storage procedure”.

8. As the investigations established the cross-border nature of the processing concerned, the CNIL informed all the European supervisory authorities on 27 August 2019, in accordance with Article 56 of the GDPR, of its competence to act as lead supervisory authority, and thus opened the procedure for the declaration of the authorities concerned in this case.
9. On 27 September 2019, the CNIL Chair submitted a draft order to the authorities concerned. Following this communication, three authorities raised relevant and reasoned objections within the meaning of Article 60 GDPR, requesting for two of them that the draft order be amended into a draft penalty, and more specifically an administrative fine for one of the two authorities. In support of this request, the authorities concerned highlighted the number of breaches, the number of data subjects, and the size of the company.
10. In order to complete its investigations, on 6 February 2020, pursuant to the aforementioned Decision No. 2018-238C, the CNIL carried out an online audit of all processing accessible from the [REDACTED] domain.
11. This audit focused more specifically on the methods of informing the data subjects on the [REDACTED] website and on the depositing of cookies on the users' terminal when they arrive on the site.
12. Following the audit, minutes No. 2018-238/2 were notified to the company [REDACTED] by letter dated 19 February 2020. The company sent the CNIL, by emails dated 4 March and 9 July 2020, the additional documents and information requested at the end of the audit.
13. On 13 January 2021, a delegation from the CNIL, pursuant to the aforementioned Decision No. 2018-238C, carried out a new online audit of any processing accessible from the [REDACTED] omain. As the company indicated that changes had been made to the way in which cookies are deposited, it was decided to carry out a new audit in order to update the findings made on 6 February 2020.
14. At the end of the audit, minutes No. 2018-238/3 were notified to the company [REDACTED] by letter dated 14 January 2021. By e-mail dated 26 January 2021, the company sent the Commission the additional documents requested during the inspection.
15. In order to examine these items, the CNIL chair appointed [REDACTED] as rapporteur on 19 December 2019, pursuant to Article 22 of the amended Act of 6 January 1978.
16. At the end of her investigation, on 2 October 2020, the rapporteur sent [REDACTED] a report detailing the breaches of the GDPR that she considered to have occurred in this case and indicating to the company that it had a period of one month in which to submit its written observations pursuant to the provisions of Article 40 of Decree No. 2019-536 of 29 May 2019.
17. This report proposed to the CNIL's restricted committee to pronounce an injunction to bring the processing into line with the provisions of articles L. 34-5 of the French Post and Electronic Communications Code (hereinafter, "CPCE"), 82 of the French Data Protection Act, and 5(1)(e), 13, 17 et 32 of the GDPR, accompanied by a penalty fine at the end of a period of three months following notification of the decision of the restricted committee as well as an administrative fine. It also proposed that this decision be made public and that the company no longer be identifiable by name upon expiry of a period of two years following its publication.

18. On 2 November 2020, through its counsel, the company submitted observations.
19. On 5 November 2020, the company was sent a notice to attend the meeting of the restricted committee on 10 December 2020.
20. On 13 November 2020, the rapporteur asked for time to respond to the observations made by [REDACTED]
[REDACTED] By e-mail of 16 November 2020, the chairman of the restricted committee informed the rapporteur that she had an additional eight days to submit her observations. By letter dated 24 November 2020, the company was informed that it had also been granted an additional period of eight days and that, as a result, the meeting of the restricted committee initially scheduled for 10 December 2020 was postponed.
21. On 16 December 2020, the company submitted further observations in response to those of the rapporteur.
22. On 11 January 2021, the CNIL sent the company a notice to attend the restricted committee meeting on 28 January 2021.
23. The company and the rapporteur presented oral observations at that meeting.
24. On 19 May 2021, a draft decision was submitted to the concerned supervisory authorities as part of the cooperation procedure, on the basis of Article 60 of the GDPR.
25. This draft decision did not give rise to relevant and reasoned objections.

II. Reasons for the decision

A. On the breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing in accordance with Article 5(1)(e) GDPR

26. According to Article 5(1)(e) of the Regulation, personal data must be “*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*
27. The rapporteur noted that, during the audit on 13 November 2018, the company told the delegation that no retention period for the personal data of customers (customers being, according to the company, holders of an account on the site who have already made at least one purchase) and prospects (holders of an account on the site who have never made a purchase) had been determined, and that it did not lawfully delete or archive such data at the end of a defined period.
28. In its defence, although it did not mention it during the audit, the company first argued that a retention period policy had been specified as early as 26 October 2018, so that it could not be accused of any breach for failure to specify retention periods.
29. In its observations of 16 December 2020, the company then indicated that the data of customers and prospects used for the purposes of marketing or managing their account was now retained in the active

database until their account is deleted or, in the event of inactivity, for three years from the last time they signed in to their account. At the end of those periods, the company specified that only the data necessary for pre-litigation or litigation purposes are archived until the date corresponding to the statute of limitations justifying their retention, after which they would be deleted.

30. Finally, at the meeting of the restricted committee and after the investigation procedure had been closed, the company produced a document intended to provide proof of the deployment of an intermediate archiving procedure and a data anonymisation process. By e-mail dated 10 February 2021, the company sent, through its counsel, a report drawn up on 5 February 2021, as well as its appendix, relating to the anonymisation process for the data of [REDACTED] s prospects and customers.
31. **According to the restricted committee**, with regard to the specification of retention periods applicable to the data of [REDACTED] 's customers and prospects, it should first be noted that the document entitled "Personal Data Retention Procedure" is dated 26 October 2018, i.e. prior to the audit. However, it was not communicated to the delegation until two months after the audit, on 5 February 2019, and on the day of the audit, 13 November 2018, the company informed the delegation that "*no retention period is implemented in the database*".
32. The restricted committee then noted that during the audit of 13 November 2018, the delegation noted the presence, in the active database, of personal data of 16,653 persons who had not placed an order in more than five years, without the company being able to provide an explanation or justification as to the length of the retention period or to provide proof of more recent contact with the said customers (exchanges with customer service, clicking on a promotional link in an e-mail, etc.). In addition, the restricted committee found that, in response to a request for additional data from CNIL, on 4 March 2020 the company provided an Excel table, which shows the retention in its database of personal data of more than 130,000 persons who have not signed in to their customer account in more than five years.
33. Consequently, while the restricted committee notes that [REDACTED] now implements retention periods, compliance with which makes it possible to comply with the provisions of Article 5(1)(e) GDPR – by guaranteeing that the data are not retained for longer than is necessary for the purposes for which they are processed – it considers, in any case, that on the day of the audit, the retention policy was not complied with and that the data was retained for excessive periods. The CNIL's supervisory delegation found that personal data were kept for much longer periods than those specified in the aforementioned document, and that those periods did not appear to be appropriate for the purposes for which the data were processed.
34. Moreover, the restricted committee considered that the company had not provided, as at the closing date of the investigation, any evidence of compliance on this point. In any event, it considers that, in accordance with Article 40 of the decree of 29 May 2019 issued for the application of the "French Data Protection Act", the information provided at the meeting of 28 January 2021 is not, as it stands, sufficient to give an opinion at this stage on whether it has been brought in compliance with Article 5(1)(e) GDPR.
35. In the light of all these elements, the restricted committee considered that the breach of Article 5(1)(e) GDPR has been established, and that the company had not completely come into compliance by the closing date of the investigation.

B. On the breach of the obligation to inform individuals pursuant to Articles 13 GDPR

36. Article 13 GDPR requires the data controller to provide, at the time the data is collected, information on its identity and contact details, that of its data protection officer, the purposes and legal basis of the processing, the recipients or categories of recipients of the personal data, transfers of personal data where

applicable, the retention period of the personal data, the rights of individuals and the right to lodge a complaint with a supervisory authority.

37. The rapporteur notes that, as it appears from the findings of the on-site inspection conducted on 13 November 2018 and the online audit of 6 February 2020, the information made available to users of the website was not complete within the meaning of Article 13 of the Regulation. In fact, certain mandatory information provided for by that Article – namely the contact details of the data protection officer, the retention periods, the legal bases of processing and certain data protection rights – were not brought to the attention of the data subjects on the [REDACTED] website, whether through the general terms and conditions of sale, the “legal and personal data notices” or the personal data retention policy.
38. In its defence, the company stated that it had made corrections in the course of the proceeding, in order to provide information that complied with the requirements of the GDPR.
39. **According to the restricted committee, firstly**, with regard to the contact details of the data protection officer, the restricted committee noted that the company acknowledged that these were not present on the [REDACTED] website until the notification of the penalty report, but specified that it was nevertheless possible to send it a request via an “unsubscribe and unregister” section within a contact form.
40. On this point, the restricted committee recalls first of all that, although it may be a useful modality, allowing customers and prospects to be put in touch with the data protection officer via a contact form dedicated to “unsubscribing and unregistering” is not a measure likely to enable compliance with the provisions of Article 13 GDPR, which requires the provision of the “contact details” for the data protection officer. Moreover, the restricted committee finds that, as at the date of the on-site inspection of 13 November 2018, the contact form was accessible from a “*Customer Service – Contact Us*” section, which, it is specified, can be used to ask “*questions about an order or for information about [the] products [of the company]*”. In such circumstances, data subjects could not spontaneously expect to be put in touch with the data protection officer to exercise their rights under the GDPR. In any event, individuals may wish to use the data protection officer’s contact details to send requests to exercise rights that are not limited to requests for unsubscribing and unregistering, such as a right of access request.
41. Under such conditions, the restricted committee therefore considers that the company breached the provisions of Article 13 GDPR.
42. The restricted committee nevertheless notes that the company had adopted measures in the context of the penalty proceeding and had demonstrated having brought into compliance its data protection policy, which now contains the contact details of the data protection officer.
43. **Secondly**, with regard to data retention periods, the company indicated that it had informed the CNIL by email on 5 February 2019 that its data retention policy had been made available to data subjects on its [REDACTED] website following the on-site inspection on 13 November 2018.
44. In this respect, the restricted committee first notes that the observations made during the inspection of 13 November 2018 attest to the absence of information on retention periods in the “legal and personal data notices”, the “general terms of sale” or any other document available on the company’s website. The restricted committee then notes that, although during the online inspection of 6 February 2020, the

delegation noted the presence of a link to a personal data retention policy, it also noted that the link was inactive. The policy was therefore inaccessible to users, as it was not otherwise available on the site.

45. Under such circumstances, the restricted committee considers that the breach of Article 13 of the GDPR is indeed demonstrated on this point, since the personal data are collected from the data subject and the information on the retention periods is among the information that must be communicated in this case, in that it makes it possible to guarantee fair and transparent processing of the personal data concerned. Thus, for example, information on retention periods allows data subjects to know how long the data are kept by the controller and, consequently, how long they can exercise their right of access.
46. The restricted committee nevertheless notes that, in the context of the penalty proceeding, the company had demonstrated having brought into compliance its data protection policy, which now contains the notices concerning retention periods for the data processed.
47. **Thirdly**, with regard to information concerning lawful bases, the company does not dispute that until 30 October 2020 no information on the lawful bases was made available to data subjects in the document entitled “Legal and personal data notices”. However, it argued that “*it cannot be blamed for a total lack of information on the legal bases insofar as some of them were available through different media*”, e.g. in the general terms and conditions of sale, and that “*compilation work was in progress at the time of the audits*”.
48. The restricted committee notes that until 30 October 2020, the data subjects were not informed of all the legal bases of the processing operations implemented. In any case, if some information was available in other documents, the restricted committee notes that it was not exhaustive, and furthermore that the accessibility and provision of information at the time of collection of the data subject’s data is a condition required under Recital 61 and Articles 12 and 13 GDPR.
49. In light of the foregoing, the restricted committee therefore considers that the company did not comply with the provisions of Article 13 GDPR.
50. The restricted committee nevertheless notes that, in the course of the penalty proceeding, the company had demonstrated having brought into compliance its data protection policy, which now presents complete information on legal bases.
51. **Fourthly**, with regard to information relating to data subject rights, the company argues that “*the lack of any mention of certain data protection rights on the [REDACTED] website results from a mere oversight and does not in any way constitute a desire on the part of [REDACTED] to prevent the exercise of certain rights by data subjects*”.
52. However, the restricted committee notes that, during the verifications carried out on 13 November 2018 and 6 February 2020, the supervisory delegation found that the company did not inform data subjects of their right to restriction of processing, to data portability and to lodge a complaint with a supervisory authority.
53. Under such circumstances, the restricted committee considers that the breach of Article 13 of the GDPR is established on this point since the personal data are collected from the data subject and the information missing in this case is among those that must be communicated in such cases. Indeed, providing information to individuals of all their rights helps to guarantee fair and transparent data processing, in

that it facilitates their exercise and thus helps to ensure that data subjects have control over the processing of their data.

54. However, the restricted committee notes that the company has demonstrated that it has brought into compliance its data protection policy, which now contains full information on the rights of data subjects. In addition, the company states that it has put a page online describing the rights of individuals under the GDPR, accessible via a link at the foot of each page of its website.
55. Consequently, the restricted committee considers that the aforementioned facts constitute a breach of Article 13 of the GDPR, but that the company had complied with all the points raised by the end of the investigation.

C. On the breach of the obligation to comply with requests to delete personal data pursuant to Article 17 GDPR

56. Under Article 17 GDPR, the data subject has the right to “*obtain from the controller the erasure of personal data relating to him or her without undue delay and the controller shall be obliged to erase such 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 which the processing is based according to point (a) of Article 6(1) (...) and 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) (...).*

57. During the inspection on 13 November 2018, the supervisory delegation was informed that when an individual requests the deletion of their account, the company does not delete the personal data but only deactivates the account in question, preventing the individual from logging in and blocking the sending of marketing messages. The delegation thus noted the presence in the database of the personal data of a customer of the company (surname, first name and e-mail address) who had previously made a request by e-mail for deletion. Access to his account had simply been disabled.
58. The restricted committee holds that it was thus established that the company did not fully comply with deletion requests.
59. The restricted committee considers that if, after a request for deletion, certain personal data of customers may be kept in intermediate storage, in particular for legal obligations or evidential purposes or when the company has an overriding legitimate ground, those not necessary in the context of compliance with such other obligations or purposes must be deleted after the exercise of this right, provided that the conditions laid down by Article 17 GDPR are met. It notes in this respect that this was at least the case for the processing of the e-mail address used for marketing purposes, since such processing is based on consent and the right to erasure is available in the event of withdrawal of consent, and that it does not appear from the elements of the proceeding that the retention of the data in question was legitimate on any other basis.

60. In view of the foregoing, the restricted committee considers that the breach of Article 17 GDPR is established.
61. However, it notes that, in the context of the penalty proceeding, the company has demonstrated having taken measures to come into compliance with Article 17 GDPR.
62. The company first demonstrated the deletion of the data of the customer who had exercised his right to erasure of data. It then stated that it had taken various measures to improve the processing of requests to exercise rights, by centralising the receipt of requests, by putting a form for exercising rights online - which can be downloaded via a direct link inserted on the information page dedicated to the rights of individuals - and by creating the e-mail address [REDACTED], dedicated to questions about personal data and managed by the company's data protection officer. In addition, the company indicated that it had developed a document containing letter templates for responding to requests to exercise rights, including a letter for responding to requests to exercise the right to erasure. Finally, the company has undertaken to set up a tracking system for requests to exercise rights in a specific tool.

D. On the breach of the obligation to ensure the security of personal data pursuant to Article 32 GDPR

63. According to Article 32 GDPR: "*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) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing[...]”.
64. **Firstly**, the rapporteur notes that at the time of the inspection on 13 November 2018, authentication when creating an account on the [REDACTED] website was based on a password composed solely of six numeric characters, of the "123456" type. The rapporteur then notes that, as regards the company's employees, the password for accessing the [REDACTED] customer relationship management software was composed of eight characters, containing at least one number and one letter. Finally, the rapporteur notes that the authentication of employees to the databases was insufficiently secure because the passwords for accessing them were stored, unencrypted, in a text file located on a company computer.
65. Firstly, the company does not dispute these facts, but maintains that the security obligation resulting from Article 32 GDPR is a best efforts obligation, not a performance obligation, so the controller's security obligation is to implement measures to reduce risks to an acceptable level, without it being compulsory, or even possible, to obtain a level of security rendering them null and void. The company also stressed that it has never suffered a personal data breach.

66. The restricted committee considers that the absence of a personal data breach is not sufficient to demonstrate the absence of an offence, nor is a data breach in itself sufficient to characterise a breach of this article. It is the task of the restricted committee to verify that the controller or, where applicable, the processor, has implemented, in accordance with this article, appropriate technical and organisational measures to prevent the risks of violation and misuse of such data. The appropriateness of the measures is assessed by verifying that the respondent has proportioned those measures, on the basis of the information available to it through reasonable diligence, to the seriousness and likelihood of the foreseeable risks, taking into account the nature and context of the data processing and the cost and complexity of the possible measures.
67. Next, the restricted committee considers that the length and complexity of a password remain basic criteria for assessing its strength. It noted in this respect that the need for a strong password is also highlighted by ANSSI.
68. For the sake of clarity, the restricted committee recalled that in order to ensure a sufficient level of security and satisfy the password strength requirements, when authentication relies solely on an identifier and password, the CNIL recommends, in its Decision No. 2017-012 of 19 January 2017, that the password have at least twelve characters - containing at least one upper-case letter, one lower-case letter, one number and one special character - or at least eight characters - containing three of these four characters - if it is accompanied by an additional measure such as, for example, the timing of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), setting up a mechanism to guard against automated and intensive attempts (e.g.: a "captcha") and/or locking the account after several failed login attempts.
69. In this case, the restricted committee considers that, in view of the rules governing their composition, the strength of the passwords accepted by the company was too weak, leading to a risk of compromise of the personal data it contains.
70. Finally, the restricted committee recalled that storing database access passwords unencrypted in a text file on a company computer is not a secure password management solution. Indeed, authentication based on the use of a short or simple password can lead to attacks by unauthorised third parties, such as "brute force" attacks, which consist of systematically testing numerous passwords in succession and thus allowing the associated accounts and the data they contain to be compromised.
71. In these circumstances, the restricted committee considers that the respondent company's password management policy was not sufficiently robust and binding to ensure data security within the meaning of Article 32 GDPR.
72. However, it notes that, in the course of the penalty proceeding, the company indicated that, with regard to customer accounts, it now requires a strong password comprising a minimum of twelve characters, including one upper-case letter, one lower case letter, one numeric character and one special character, which was corroborated by a screen print. For employees, the company has implemented a strong password on access to [REDACTED] Concerning the storage of database access passwords in an unencrypted file, the company demonstrated having discontinued the practice and that it has implemented a secure password management solution by subscribing to the [REDACTED] solution, which guarantees encrypted password storage.

73. **Secondly**, the rapporteur notes that the hash function used for the storage of passwords of employees using the [REDACTED] website was obsolete (MD5).
74. In its defence, the company did not contest these facts, but repeated the same argument on the best-efforts obligation.
75. The restricted committee recalls that the use of the MD5 hash function by the company has not been considered state of the art since 2004 and its use in cryptography or security is prohibited. Thus, the use of this algorithm would allow a person with knowledge of the hashed password to decrypt it without difficulty in a very short time (e.g. by means of freely accessible websites that allow the value corresponding to the password hash to be retrieved).
76. In these circumstances, in view of the risks incurred by the individuals mentioned above, the restricted committee considers that the hash system used did not make it possible to guarantee the security of the data, within the meaning of Article 32 GDPR.
77. However, it notes that, in the context of the penalty proceeding, the company demonstrated having implemented a satisfactory hashing system, in SHA256, of all users' passwords.
78. **Thirdly**, the rapporteur notes that the company's employees had access to a copy of the [REDACTED] production database through an account shared by four employees.
79. In its defence, the company did not contest these facts, but repeated the same argument on the best-efforts obligation.
80. The restricted committee recalls that the attribution of a unique identifier per user and the prohibition of shared accounts are among the indispensable precautions to guarantee effective traceability of access to a database. In this case, the sharing of the account allowing access to the copy of the production database by four employees does not make it possible to guarantee proper authentication of users and, consequently, effective management of accreditations and proper traceability of access. Such a lack of traceability of access does not allow the identification of fraudulent access or the author of any deterioration or deletion of personal data.
81. In these circumstances, the restricted committee considers that the use of a generic account does not guarantee data security within the meaning of Article 32 GDPR.
82. However, it notes that, in the context of the penalty proceeding, the company demonstrated having taken measures by setting up an authentication system for accredited users.

E. On the breach of obligations relating to information (cookies) stored on users' electronic communications terminal equipment, in accordance with Article 82 of the French Data Protection Act

[Offence not subject to cooperation on which the supervisory authorities concerned do not have to take a position.]

83. Article 82 of the French Data Protection Act requires that users be informed and that their consent be obtained before any registration or access to information already stored in their equipment. Any deposit of cookies or other trackers must therefore be preceded by the information and consent of the persons concerned. This requirement does not apply to cookies whose "exclusive purpose is to enable or

facilitate electronic communication”, or those “strictly necessary for the provision of an online communication service at the express request of the user”.

84. The rapporteur considers that the company did not comply with these provisions since it emerged from the online inspections of 6 February 2020 and 13 January 2021 that, on arrival at the [REDACTED] website, several cookies that did not fall within the scope of the two exceptions mentioned above were deposited on the user’s terminal as soon as they arrived on the site’s home page, and before any action on their part.
85. The company does not dispute these facts.
86. In fact, the restricted committee notes that it emerged from the findings of the online inspection of 6 February 2020 that thirty-two cookies were automatically deposited as soon as the user arrived on the site’s home page, and before any action was taken by the user. In response to a request for further information from the CNIL, the company indicated on 4 March 2020 that the purposes of the cookies deposited were to have “*better knowledge of customers*”, “*better advertising targeting*” and to personalise “*the offering and promotional operations*”.
87. The restricted committee also noted that, even though the company had stated, in its observations in response of 16 December 2020, that it had “*stopped, since 10 November 2020 automatic depositing cookies subject to consent*” when users arrived on its site, the delegation noted, during the online inspection of 13 January 2021, the deposit of thirteen cookies upon arrival on the website. By e-mail dated 26 January 2021, the company sent the additional documents requested during the inspection and confirmed, in particular, that some of the cookies deposited were for advertising purposes.
88. Consequently, since the cookies deposited were not exclusively for the purpose of allowing or facilitating electronic communication and were not strictly necessary for the provision of the service, the company is required to obtain the consent of users prior to their deposit.
89. The restricted committee therefore considers that there has been a breach of Article 82 of the French Data Protection Act.
90. However, the restricted committee emphasised that the company had made significant changes to its website during the penalty proceeding, and that the cookies for which users’ consent was required were no longer automatically deposited on the user’s terminal when they arrived on the site’s homepage since 26 January 2021.

F. On the breach of the obligation to gather consent from the data subject of a direct marketing operation using an electronic communications system in accordance with Article L. 34-5 CPCE

[Offence not subject to cooperation on which the supervisory authorities concerned do not have to take a position.]

91. According to Article L. 34-5 CPCE: “*Direct marketing by means of automated electronic communication systems within the meaning of Article L. 32, 6°, is prohibited, by fax or electronic mail using the contact details of a natural person, subscriber or user, who has not expressed their consent prior to receiving direct marketing by this means.*

For the application of the present article, consent shall mean any expression of free, specific and informed intent whereby a person agrees that personal data related to them is used for direct marketing purposes. [...]

However, direct e-mail marketing is authorised if the recipient's contact details have been collected from them, in compliance with the provisions of French Data Protection Act No. 78-17 of 6 January 1978, in connection with a sale or provision of services, if the direct marketing concerns products or services similar to those previously provided by the same natural person or legal entity, and if the recipient is offered, expressly and unambiguously, the opportunity to object, without charges, other than those related to the transmission of the refusal, in a simple manner, to the use of his/her contact details at the time they are collected and every time a marketing e-mail is sent to them if they have not initially refused such use".

92. The rapporteur notes that during the inspections carried out on 13 November 2018 and 6 February 2020, the delegation found that, when an account was created without a purchase being made on the company's website, no procedure for obtaining consent to the collection and processing of personal data for the purpose of marketing by e-mail was implemented.
93. In its defence, the company argued that because of the information on the site, individuals who had created an account could not have been unaware that the company would regularly send them commercial communications by e-mail. It also recalls that in order to validate a registration when creating an account on the company's website, the person must accept the company's general terms and conditions of sale, which provide that their personal data will be used by the company to inform them by e-mail of upcoming sales and special offers.
94. The restricted committee considers that the creation of an account does not prejudge the eventual ordering of products from the company [REDACTED]. The restricted committee considers that, in the absence of purchases, the company cannot validly plead the benefit of the exception created by Article L. 34-5 CPCE allowing marketing without prior consent when the recipient's contact details have been collected from them in connection with a sale or provision of services and if the direct marketing concerns products or services similar to those provided by the same natural person or legal entity.
95. Consequently, the restricted committee considers that the company was required to obtain the free, informed, specific prior consent of persons creating an account on its website without having made a purchase, to receive direct marketing messages by e-mail, in accordance with Article L. 34-5(1) CPCE.
96. In these circumstances, the restricted committee considers that the breach of Article L. 34-5 of the CPCE is established.

In the course of the proceeding, the company demonstrated having inserted a checkbox on the online account creation form to allow for specific and unambiguous consent to be taken into account for persons wishing to create an account in the future.

97. For individuals who already had an account on the [REDACTED] website, the company says it plans to send marketing emails only to those who have already made a purchase on its site. It also reported that it had sent emails to obtain the consent of 549 prospects who had not yet given their consent to receive electronic marketing messages or made a purchase following the creation of their account.

98. During the meeting of the restricted committee, the company also specified that in order to comply with the provisions of Article L. 34-5 CPCE, it intended to send each prospect who had not yet given their consent five e-mails aimed at obtaining their consent to receive electronic marketing. Those five emails would be sent within a period of 100 days from the date of the prospect's last activity. The company indicated that after 100 days of inactivity on the part of the prospect and without the latter's consent to receive marketing messages following the five e-mails it had sent to them, it would stop marketing to them.
99. The restricted committee considers that the fact of soliciting the persons in question to ask them if they wish to receive marketing e-mails constitutes in itself a processing operation which cannot be based, in this case, on any legitimate interest of the company. It is clear from the documents in the file that, by choosing to create an account on the company's website in order to access its offers, the prospective customers have shown a certain interest in the services offered by the company and that they can therefore reasonably expect the company to contact them. However, it considers that sending prospects five emails, let alone over a period of 100 days, exceeds the number of emails they could reasonably expect to receive.
100. In these circumstances, the restricted committee considers that the company has not been brought in full compliance by the closing date of the investigation.

III. On corrective powers and their publication

101. Under the terms of Article 20 III of the amended Act of 6 January 1978:

“When the controller or his processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chair of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the restricted committee of the CNIL with a view to the announcement, after adversarial procedure, of one or more of the following measures: [...]”

2. An injunction to bring the processing into compliance with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law or to comply with the requests made by the data subject to exercise his/her rights, which may be accompanied, except in cases where the processing is implemented by the State, with a penalty fine not exceeding 100,000 euros per day of delay from the date fixed by the restricted committee; [...]”

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83.”

Article 83 GDPR states that “*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive*”, before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

102. **Firstly**, on the principle of imposing a fine, the company maintains that such a measure is not justified. It points out in particular that it has never been condemned by the restricted committee, that the aforementioned breaches do not in any way constitute a deliberate breach of the GDPR, that the data subjects have not suffered any damage, that no specific data referred to in Articles 9 and 10 GDPR is concerned, that it has cooperated in good faith with the CNIL throughout the procedure and that it has taken measures to bring itself into compliance.
103. The rapporteur recalls that in determining the amount of an administrative fine, the restricted committee must take into account the criteria specified in Article 83 GDPR, such as the nature, gravity and duration of the infringement, the measures taken by the controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority and the categories of personal data concerned by the infringement.
104. Firstly, the restricted committee considers that the company has demonstrated gross negligence with regard to the fundamental principles of the GDPR, since six breaches have been found, particularly of the principle of limiting the data retention period, the obligation to inform data subjects of the processing of their personal data and the obligation to respect their rights.
105. The restricted committee then noted that several breaches found concerned a significant number of individuals, namely [REDACTED] users in France, [REDACTED] in Spain, [REDACTED] in Italy and [REDACTED] in Portugal.
106. Finally, the restricted committee notes that the compliance measures put in place following the notification of the penalty report do not concern all the breaches and do not exonerate the company from its responsibility for the past, in particular in view of the breaches observed,
107. Consequently, the restricted committee considers that an administrative fine should be imposed in view of the breaches of Articles 5(1)(e), 13, 17 and 32 GDPR, 82 of the French Data Protection Act and L. 34-5 of the CPCE.
108. **Secondly**, with regard to the amount of the fine concerning breaches of the GDPR, the restricted committee recalls that Article 83(3) GDPR provides that in the event of multiple breaches, as in the case in point, the total amount of the fine may not exceed the amount set for the most serious breach. Insofar as the company is alleged to be in breach of Articles 5(1)(e), 13, 17 and 32 GDPR, the maximum fine that can be imposed is 20 million euros or 4% of annual worldwide turnover, whichever is higher.
109. With regard to the amount of the fine relating to the breach of Article 82 of the French Data Protection Act and Article L. 34-5 CPCE, the restricted committee recalls that with regard to breaches of provisions originating in texts other than the GDPR, as is the case with Article L. 34-5 CPCE, which transposes into domestic law the “ePrivacy” Directive, Article 20, paragraph III, of the “French Data Protection Act” gives it the competence to impose various penalties, in particular an administrative fine, the maximum amount of which may be equivalent to 2% of the total annual worldwide turnover of the previous financial year generated by the controller. Furthermore, the determination of the amount of this fine is assessed in light of the criteria specified in Article 83 GDPR.
110. The restricted committee also recalls that administrative fines must be dissuasive but proportionate. In particular, it considers that the company’s activity and financial situation must be taken into account when determining the penalty and, in particular, in the case of an administrative fine, its amount. In this

regard, it notes that the company reports turnover from 2018 to 2020 of approximately [REDACTED] euros, then approximately [REDACTED] euros and finally approximately [REDACTED] euros, for a net profit of [REDACTED] euros, then [REDACTED] euros and finally [REDACTED] euros, respectively. Consequently, the amount proposed in the report is far from reaching the maximum amount of financial penalty stipulated by the GDPR since it represents only [REDACTED] % of the company's turnover. In view of these elements, the restricted committee considers that the imposition of a fine of 500,000 euros appears justified, i.e. 300,000 euros for the breaches of Articles 5(1)(e), 13, 17 and 32 GDPR and 200,000 euros for the breaches of Article 82 of the French Data Protection Act and Article L. 34-5 CPCE.

111. **Thirdly**, an injunction to bring the processing into compliance with the provisions of Article 5(1)(e) GDPR and Article L. 34(5) CPCE was proposed by the rapporteur when the report was notified.
112. The company argues that the actions it has taken in relation to all the breaches identified should lead to the Rapporteur's proposal for injunctions not being followed.
113. With regard to the breach of the obligation to define and respect a retention period for personal data proportionate to the purpose of the processing pursuant to Article 5(1)(e) GDPR, the company indicated that it had implemented an internal procedure for archiving and then anonymising the data.
114. However, the restricted committee considered that the company had not provided, as at the date of the close of the investigation, any information enabling it to attest to compliance on this point. In any case, it considers that the information provided during the session is not sufficient to decide at this stage whether it will comply with Article 5(1)(e) GDPR.
115. With regard to the breach of the obligation to obtain the consent of the data subject of a direct marketing operation by means of an automated electronic communications system pursuant to Article L. 34-5 CPCE, the restricted committee considers that the company has taken satisfactory measures to obtain the consent of persons when creating an account on the [REDACTED] website. The restricted committee also noted that the company had undertaken, in the course of the procedure, to stop sending direct marketing messages by e-mail to prospective customers without their prior consent. However, it considers that it has not demonstrated full compliance with Article L. 34-5 CPCE insofar as it intends to seek the consent up to five times of persons who have created an account in the past. Consequently, the restricted committee considers that an injunction should be imposed on this point.
116. **Fourthly**, the restricted committee considers that the publication of the penalty is justified in view of the plurality of breaches identified, their persistence, their seriousness and the number of data subjects.

FOR THESE REASONS

The CNIL's restricted committee after having deliberated, intends to decide to:

- Impose an administrative fine on [REDACTED] in the amount of 500,000 (five hundred thousand) euros for all the breaches found, which breaks down as follows:
 - **300,000 (three hundred thousand) euros** for breaches of Articles 5(1)(e), 13, 17 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "GDPR");
 - **200,000 (two hundred thousand) euros** for breaches of Article 82 of the amended French Data Protection Act of 6 January 1978, and of Article L. 34-5 of the French Post and Electronic Communications Code (hereinafter "CPCE");
- Issue an injunction against [REDACTED] to bring the processing operations into compliance with the obligations resulting from Articles 5(1)(e) GDPR and L. 34-5 CPCE, and in particular:
 - **With regard to the breach of the principle of limiting the retention period of personal data, specify and implement a personal data retention policy which does not exceed the period necessary for the purposes for which it is collected and processed, and in particular:**
 - Stop retaining the personal data of former customers of the company's website after a fixed period of inactivity, purge such data retained by the company up to the date of the restricted committee's decision, and provide proof of the deletion of such personal data beyond a specific inactivity period, which the company is responsible for proving;
 - Provide proof that a procedure has been set up for the intermediate archiving of customers' personal data, after having sorted the relevant data to be archived and deleted the non-relevant data, and provide proof of the starting point of this archiving (e.g. invoices archived for accounting purposes);
 - **With regard to the breach of the obligation to obtain the consent of the individual data subject concerned by a direct marketing operation by means of an automated electronic communications system:** cease marketing to non-customers who have not expressed their consent, unless their consent is obtained;
- Attach to the injunction a penalty fine of 500 (five hundred) euros per day of delay at the end of a period of three months following notification of this decision, with proof of compliance to be sent to the restricted committee within this period;
- Make public, on the CNIL website and on the Légifrance website, its decision, which will no longer identify the company at the end of a period of two years following its publication.

The Chairman

Alexandre LINDEN

Summary Final Decision Art 60

Notification

Administrative fine, Compliance order

EDPBI:FR:OSS:D:2021:279

Background information

Date of final decision: 14 June 2021

Date of broadcast: 21 September 2021

LSA: FR

CSAs: BE, ES, IT, PT

Legal Reference: Article 5 (Principles relating to processing of personal data), Article 13 (Information to be provided where personal data are collected from the data subject), Article 17 (Right to erasure), Article 32 (Security of processing)

Decision: Administrative fine, Compliance order

Key words: Data retention, Transparency, Right to erasure, Data security, Password

Summary of the Decision

Origin of the case

The LSA carried out an own volition audit at the premises of the controller in order to verify its compliance with all the provisions of the GDPR. The audit focused on the processing of personal data relating to the company's customers and prospective customers. More specifically, the LSA investigated on the information provided to data subjects, compliance concerning data subject requests and data retention periods.

In order to complete these investigations, the LSA also carried out an online audit relating to all processing accessible from the controller's website, with a particular focus on, *inter alia*, the methods used for informing data subjects.

Findings

In the course of its investigation, the LSA noted that the active database of the controller contained personal data of 16.653 persons who had not placed an order in more than 5 years and 130,000 persons who have not signed in to their customer account in more than 5 years. In this regard, the LSA

ruled that, although the controller implemented a retention period policy, personal data were kept for much longer periods than those specified in this policy on the day of the audit and did not appear to be appropriate for the purposes for which the data were processed (Article 5(1)(e) GDPR).

Furthermore, following its on-site and online audits, the LSA founds that certain mandatory information provided for by Article 13 GDPR was missing, namely the contact details of the DPO, the data retention periods, the legal bases of the processing and information on certain data protection rights. Nonetheless, the LSA noted that the company had complied with all the point raised regarding the information of data subjects by the end of the investigation.

As to the controller's obligation to comply with requests to delete personal data (Article 17 GDPR), the LSA found that when an individual requested the deletion of its account, the company simply deactivated the account in question. In this regard, the LSA stressed that the email address used for marketing purposes should have been deleted in the event of withdrawal of consent insofar as its retention is not legitimate on any other basis. Measures were taken by the company in the course of the procedure but did not fully achieve compliance, so the LSA issued an injunction against the company.

Finally, the LSA found that the passwords format when both creating an account on the controller's website and accessing to the customer databases were insufficiently robust to ensure data security within the meaning of Article 32 GDPR (Security of processing). Violations of the same Article have been reported by the LSA due to the obsolete nature of the hash function used for the storage of passwords of employees using the controller's website and the use of the same account by several employees when accessing to a copy of the controller's production database.

Decision

The LSA imposed an administrative fine of 300,000 euros to the controller to be in breach of Articles 5(1)(e), 13, 17 and 32 GDPR

In addition, the LSA imposed a compliance order on the controller to remedy its breach of Article 5(1)(e) with a penalty payment of 500 euros per day of delay at the end of a period of 3 months following notification of the decision.

Decision No. MED 2021-089 of 16 September 2021 issuing an order to the company [REDACTED]

(MDM No. 211104)

The Vice Chairman of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Decision No. 2013-175 of 4 July 2013 adopting the rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2018-202C of 28 September 2018 of CNIL's Chair to instruct the secretary general to carry out or have a third party carry out an assignment to verify the processing implemented via the [REDACTED] domain or related to personal data collected by it, through any organisation that may be concerned by the use of such data;

Having regard to the online findings report No. 2018-202/1 of 1 October 2018 and No. 2018-202/2 of 11 February 2020;

Having regard to the hearing report No. 2018-202/3 of 3 March 2020;

Having regard to the other documents in the file;

I. Background and procedure

Created in 2009, the company [REDACTED] located at [REDACTED] [REDACTED], is a limited liability company specialising in the rental of holiday homes and apartments abroad, mainly in Spain. It recently developed its activities in France, Italy and Portugal. The company has [REDACTED] employees and generated turnover of [REDACTED].

The company publishes the website [REDACTED] and connects rental agencies with individuals. Those agencies pay the company a commission for reservations made using the [REDACTED] website. In 2018, 1275 reservations were made.

The [REDACTED] domain is divided into several subdomains, the versions of which are identical:

- [REDACTED] is the French version of the website;
- [REDACTED] is the Spanish version;
- [REDACTED] is the English version of the site.

In 2018, CNIL received an internal report, informing it that files containing personal data and unencrypted passwords are allegedly freely accessible and downloadable without prior authentication on the website, [REDACTED]

Pursuant to the Decision No. 2018-202C of 28 September 2018 of the CNIL Chair, a delegation carried out two online verification missions on 1 October 2018 and 11 February 2020, in order to verify the compliance of any processing accessible from the domain [REDACTED] or concerning personal data collected from it from any organisation concerned by their implementation under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the Regulation or the GDPR) and the amended Act of 6 January 1978 (French Data Protection Act). These two verification missions were followed by a hearing on 3 March 2020, followed by a questionnaire sent to the company on 27 May 2020.

In the context of on-line verifications, this included checking the information procedures for provision of information to individuals and data security. The hearing and questionnaire made it possible to clarify the findings made during the inspections. Additional information was provided by the company on 3 and 18 October 2018, as well as on 10 March and 18 June 2020.

On 6 July 2021, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

That draft decision did not give rise to any relevant and reasoned objections.

II. Breaches with regard to the provisions of the GDPR

A breach of the obligation to collect data for specified, explicit and legitimate purposes

Article 5(1)(b) of the GDPR provides that personal data must be collected “*for specified, explicit and legitimate purposes*”.

The delegation was informed by the company that it collects email addresses via a “newsletter” field on the home page of the [REDACTED] website. The delegation noted that 263 email addresses collected from the “newsletter” field are present in the database.

However, the company stated that it no longer used that data, insofar as it does not send any newsletter or advertising to prospects.

By collecting personal data that it does not use, the company collects data for no purpose, in breach of Article 5(1)(b) of the Regulation. It is therefore up to the company to stop the collection of email addresses via the “newsletter” field and delete the email addresses previously collected via that field.

Breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing

Article 5(1)(e) of the GDPR provides that personal data must be “*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*”.

The CNIL recalls that the retention period of personal data must be determined according to the purpose pursued by the processing. Where the data is no longer necessary for the purpose for which it was collected, the data must either be deleted, or be subject to intermediate archiving when the data is necessary for compliance with legal obligations or for pre-litigation or litigation purposes. The data thus placed in intermediate archiving are then archived for a period not exceeding that necessary for the purposes for which they are stored, in accordance with the provisions in force. Thus, after having carried out a sorting of relevant data to be stored, the data controller must provide for this purpose a dedicated archive database or logical separation in the active database. This logical separation is ensured by the implementation of technical and organisational measures ensuring that only persons with an interest in processing the data due to their duties can access them. Beyond such data retention periods in intermediate archive, personal data must, unless otherwise provided, be deleted or anonymised.

Thus, in the context of commercial activities, customer and prospective data may be reasonably retained for a period of three years from the end of the business relationship, considered as the last purchase or contact from the user. At the end of this period, the CNIL recommends that such data be deleted.

First, the delegation was informed that the client data was kept for ten years because they are linked to reservation contracts to be retained for such a period for tax and accounting purposes. At the end of that period, the company carries out a “cleaning” of the data in order to keep only the name of the users. The company informed the delegation that it retains the names of users indefinitely in order to have a means of searching in its database in case of administrative or commercial need.

In this respect, the delegation noted that the names of 10,730 customers whose last reservation was over ten years ago were retained without a time limit.

However, the CNIL recalls that a retention period must be set according to each purpose and that under no circumstances must personal data be kept for an indefinite period.

Thus, the retention of the names of the company's customers beyond ten years and for an indefinite period is excessive with regard to the purposes related to administrative or commercial needs.

Secondly, the delegation was informed that the company retains the data of prospects for a period of five years, “*fixed arbitrarily*”. In this context, prospects are those who have started a reservation process without finalising it or having issued an accommodation selection request. The company has specified that this retention was for the purpose “*of internal commercial use, in order to better target our responses to new selection requests from customers*”.

However, the fixed retention period must be necessary with regard to the purposes for which the personal data are processed. The retention of such individuals' data for five years for “*internal commercial use*” appears to be excessive, since the company can improve its offers by studying unfinished and anonymous requests.

Thirdly, the delegation was also informed that no procedure for the intermediate archiving of customer data or access restriction was implemented within the company.

All of these facts constitute a breach of Article 5(1)(e) of the GDPR. It is therefore up to the company to set data retention periods for its customers and prospects that are proportionate to the purposes for which such data was collected. It is also up to it to implement an intermediate archiving procedure for its customers' data, with restricted access.

A breach of the obligation to inform persons

Firstly, Article 12 of the GDPR provides that “*The controller shall 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*”.

With regard to the transparency of information, the guidelines of the “Article 29” Working Party (now the European Data Protection Board) on transparency within the meaning of Regulation (EU) 2016/679, adopted on 29 November 2017, specify, concerning information, that the information “*This information should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use. In an online context, the use of a layered privacy statement/ notice will enable a data subject to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text searching for particular issues (...)*”. The Guidelines add that “*The data subject must not have to actively search for information covered by [Articles 13 and 14] amongst other information, such as terms and conditions of use of a website [...]*”.

However, the delegation found that the information of individuals relating to the processing of their personal data is contained in the “Terms of Service” (“TOS”) of the [REDACTED] website, among other information not related to personal data protection.

Therefore, the procedures for providing information on personal data protection do not meet the transparency requirements laid down in the Regulation.

Concerning the accessible nature of the information, the aforementioned guidelines also state that “*The ‘easily accessible’ element 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, [or] by linking them to it*”.

These guidelines illustrate the need for the data controller to take concrete measures to ensure that the information is provided directly to the data subject or to actively direct that person to the location of such information.

However, the delegation found that the information relating to personal data collected during the creation of a user account was not easily accessible. Indeed, although as part of the Terms of Service located at the bottom of the [REDACTED] website, this information is not directly brought to the attention of the data subjects, whether on the website's collection pages or via a clickable link inserted on the collection page referring to a document containing that information.

It follows from the above that both transparency and accessibility of the information provided to the data subjects are lacking in the present case.

Secondly, Article 13 of the GDPR provides that different information is provided to the data subject at the time of the collection of personal data concerning them.

However, the delegation found that the following mandatory information was absent from the Terms of Service of the [REDACTED] website:

- The existence of the right to ask the data controller to limit data processing associated with a data subject, the right to object to processing, and the right to data portability;
- Data retention periods;
- The right to lodge a complaint with a supervisory authority;
- The legal basis for processing.

All of these facts constitute a breach of Articles 12 and 13 of the Regulation. It is therefore up to the company to include the information required by Article 13 of the Regulation in a dedicated medium, such as a privacy policy, and to bring such information to the attention of the users of its website, either directly on the personal data collection pages or by means of a clickable link to the privacy policy. The latter must also be supplemented in order to contain all the information required by Article 13 of the Regulation.

A breach of processing obligations

Article 28 of the Regulation provides that the processing carried out by a processor for a data controller is governed by a contract which determines the conditions under which the processor undertakes to carry out the processing operations on behalf of the data controller.

In accordance with Article 28 of the Regulation, that contract specifies the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data, and the categories of data subjects, and the data controller's rights and obligations. That contract must in particular provide that the processor only processes personal data on documented instructions from the data controller.

In this case, [REDACTED] is responsible for hosting the [REDACTED] website and for server management, while [REDACTED] is the [REDACTED]'s payment provider. In this context, they process personal data on behalf of [REDACTED]. As such, these two companies are processors of [REDACTED] within the meaning of Article 4 of the GDPR.

However, the delegation found that the service contracts binding these two service providers to [REDACTED] did not contain any of the provisions required by Article 28 of the GDPR.

These elements combined constitute a breach of Article 28 of the GDPR. It is therefore up to the company to supplement the contracts concluded with its processors in order to include all the information required by this article, which specifies the obligations incumbent upon them in terms of the protecting the security and confidentiality of your customers' data.

A breach of the obligation to ensure the security and confidentiality of personal data

Article 32 of the Regulation provides in particular that "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

Firstly, the delegation was informed that the production data, which correspond to actual data, were imported three to four times a year into the database for testing.

However, the CNIL considers that the use of fictitious or anonymised data in the context of IT testing constitutes an essential security precaution to be adopted in terms of IT developments.

Secondly, the company has set up a password hash for the user accounts of the [REDACTED] website using the MD5 + salt algorithm.

However, the CNIL recommends using hashing algorithms deemed strong for the storage of passwords, with the MD5 + salt function being deemed obsolete (Decision No. 2017-012 of 19 January 2017 adopting a recommendation on passwords).

Thirdly, the delegation found that a user account could be created on the [REDACTED] website using a password consisting of a single character. No complex password rules or additional measures have been put in place.

Similarly, in the context of the hearing of 3 March 2020, the company stated that access to the new development server [REDACTED] was obtained by means of a password consisting of 8 characters, including 2 different types of characters (lower case and number) and that no additional measures were put in place.

However, the password characteristics defined by the company do not ensure a sufficient level of personal data security. Indeed, authentication based on the use of an insufficiently complex password can lead to the compromising of the associated accounts and attacks by unauthorised third parties, for example “brute force” attacks which consist of systematically testing many passwords successively.

In this respect, the CNIL's decision on passwords recommends that passwords consisting of 8 characters contain 3 of the 4 character types (upper case letters, lower case letters, numbers, and special characters) and be accompanied by an additional measure such as the timing out access to the account after several failures or an account locking measure after a maximum of ten unsuccessful login attempts.

Fourthly, the delegation found that the current production database is based on an obsolete version (mySql, October 2010), which is no longer subject to security updates in case of vulnerability.

However, the CNIL recommends that regular monitoring and updating of the technical and application components be carried out, particularly on websites, servers, databases, and workstations.

All of these facts constitute a breach of Article 32 of the GDPR. It is therefore up to the company to stop using actual data in the context of IT testing, to use a hashing algorithm deemed strong for the storage of passwords, to define password complexity rules for users of its site to ensure a sufficient level of security of their personal data and to regularly update the database of technical and application components.

Consequently, [REDACTED], located at [REDACTED] is hereby ordered, within 3 months of notification of this Decision, and subject to any measures it may have already adopted, to:

- **only process personal data for specific, explicit and legitimate purposes**, particularly by ceasing to collect email addresses via the "newsletter" field on the homepage of the [REDACTED] website, and by deleting the email addresses previously collected;
- **define and implement a data retention period policy relating to the company's customers and prospects which does not exceed the duration necessary for the purposes for which they are collected**, and implement an effective procedure for archiving the processed data with restricted access;
- **inform the data subjects**, in accordance with the provisions of Articles 12 and 13 of the Regulation, about the personal data processing put in place, particularly by providing users:
 - complete information, in a dedicated document, on the personal data processing implemented;
 - transparent and directly accessible information on the forms from which personal data are collected;
- **provide in all contracts between the company and its service providers**, in particular [REDACTED] and [REDACTED], clauses specifying the obligations incumbent on the service providers with regard to protecting the security and confidentiality of the company's customers' data, and specifying in particular that service providers may act only on instructions from the controller, in accordance with Article 28 of the Regulation;
- **to take all security measures, for all personal data processing operations, to protect the security of such data and prevent unauthorised third parties from accessing it pursuant to Article 32 of the GDPR, and in particular:**
 - **with regard to the production data imported into the development database in order to conduct testing:**
 - cease using actual personal data for the development and testing phases;
 - **with regard to passwords:**
 - for instance, passwords consist of a minimum of 12 characters, containing at least one upper case letter, one lower case letter, one number, and one special character; **or**
 - passwords are composed of at least 8 characters, containing 3 of the 4 character types (upper case letters, lower case letters, numbers, and special characters) **and** are accompanied by a supplemental measure such as timing out access to the account after several failures (temporary access suspension whose duration increases as attempts are made), the establishment of a mechanism to guard against automated and intensive submission of attempts (for example: "captcha") and/or the locking the account after several unsuccessful authentication attempts (maximum 10);

- use a recognized and secure algorithm, such as for example bcrypt, scrypt or PBKDF2, and, where applicable, the use of a salt, for the storage of passwords in the database;
- **regularly monitor and update** the technical and application components on websites, servers, database, workstations, etc.;
- **Provide supporting documentation to the CNIL that all of the aforementioned claims have been complied with within the time limit set.**

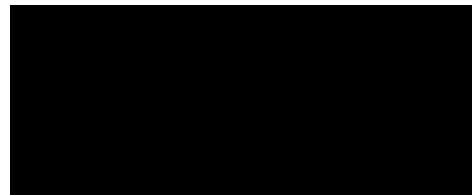
At the end of that period, if [REDACTED] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if [REDACTED] has not complied with this order by the end of that period, a rapporteur will be appointed who may request the restricted committee to issue one of the sanctions provided for by Article 20 of the amended Act of 6 January 1978.

The Vice-President

[REDACTED]

The Chair



Paris, on

01 OCT. 2021

Registered letter with acknowledgement of receipt

AR No: [redacted]

Ref. No. : MLD/LCN/RAL211029

Referral no. 21008089

(to be quoted in all correspondence)

Dear Sir,

I am following up on the various exchanges that have taken place between the services of the *Commission Nationale de l'Informatique et des Libertés* ("CNIL" - French Data Protection Authority) and the Data Protection Officer of [redacted] as part of the investigation of [redacted]; complaint sent to CNIL by the Austrian authority for the protection of personal data pursuant to Article 56.1 of the General Data Protection Regulation ("GDPR").

[redacted] had lodged a complaint with his national data protection authority against [redacted] concerning difficulties in exercising his right to erasure.

The failures noted at the time of the exchanges between CNIL and [redacted] lead me, in agreement with the other European data protection authorities concerned by the processing implemented, to remind [redacted] of its obligations, in accordance with the provisions of article 58.2.b) of the GDPR.

In this case, the complainant, holder of the email address [redacted] sent an account deletion request by email on 6 March 2021 which went unanswered. Subsequently, the complainant made a follow-up via a "support ticket" dated 2 April 2021 for which he was informed that he had to wait for the response from the team dedicated to the protection of personal data. Indeed, the "support" team had no indication of these procedures.

[redacted] indicates that it has deleted the account of [redacted] but that it only informed him on 25 June 2021.

RÉPUBLIQUE FRANÇAISE

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

However, I remind you that in accordance with the provisions of article 12.3 of the GDPR, the data controller is required to respond to the person who made a request in application of articles 15 to 22 of the GDPR, indicating the measures taken as a result of his request as soon as possible "*and in any event within one month of receipt of the request.*"

Therefore, I call you to order by this letter on **the need to respond to people making a request to exercise their rights within the legal period of one month, which may be extended by two months if necessary, in particular in the event of the complexity of the request.**

Finally, I would like to point out that this decision, which closes the investigation of [REDACTED] [REDACTED]'s complaint, does not exclude the CNIL from making use, particularly in the event of new complaints, of all the other powers attributed to it by the GPDR and by the amended Act of 6 January 1978.

Yours sincerely,



Marie-Laure DENIS

The Chair



Reg. letter no. 2C 127 846 0299 8

Paris, on

References to be quoted in all correspondence:

Our ref.: JDE/ACB/RGL/MDM171026 – CTX-2017-053

Dear Sir,

I refer to the complaint lodged by [REDACTED] with the Netherlands data protection authority, which the latter forwarded to the CNIL pursuant to Article 56.1 of the General Regulation on the protection of personal data. This complaint concerned the complainant's inability to obtain erasure of the geolocation data linked to his account on the [REDACTED] application from [REDACTED]

The CNIL notes that the processing undertake by [REDACTED] is founded on the contractual basis (article 6(1) (b) GDPR), as it is mentioned in your privacy policy.

Considering that, for the performance of the contract between [REDACTED] and the complainant, the retention of geolocation data is necessary to provide the service offers by [REDACTED] it appears that the deletion of the data required by the complainant was not possible as long as the contract between [REDACTED] and the complainant was undergoing.

To the extent that only the termination of the contract would render possible the deletion of the complainant' geolocation data, it appears that the proposition made by [REDACTED] to the complainant to delete its account was appropriate.

In any case, I note that following exchanges between [REDACTED] and the complainant, he agreed to reset his account so that the data relating to his geolocation would be deleted. I note that this reset occurred on 17 December 2020.

Consequently, I decided to close the procedure related to the aforementioned complaint.

Please do not hesitate to contact the Commission ([REDACTED]
[REDACTED]) if you require any further information.

Yours faithfully,

Marie-Laure Denis

The President

Registered letter with AR

N° : 2C1376091466A



Paris, on

02 NOV. 2021

Our Ref.: [REDACTED] RAL211042

Cases n° 19011346, n° 19016027, n° 19016065
(to be referenced in all correspondence)

Dear Sir,

This is further to the exchanges that took place between the CNIL's services and [REDACTED]
[REDACTED], then Data Protection Officer (DPO) of [REDACTED]
[REDACTED], in the framework of a first complaint which has been 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).

This complaint (case n° 19011346) was lodged by [REDACTED] a German customer of [REDACTED] who had noticed several security flaws concerning the processing of personal data linked to your term deposit activity.

Two other complaints relating to the same facts and the same processing were subsequently transmitted to us by the data protection authority of Rhineland-Palatinate concerning other German customers, [REDACTED] (case n° 19016027) and [REDACTED] (case n° 19016065).

The complainants state that they received unencrypted or weakly encrypted e-mails confirming the opening of term deposit accounts, making their name, address, account number and the amount deposited easily accessible.

The exchanges that have taken place between the CNIL departments and the [REDACTED]'s DPO lead me, in agreement with the other European data protection authorities concerned by the data processing, to reprimand [REDACTED] in accordance with the provisions of Article 58.2.b) of the GDPR.

Indeed, I would remind you that, as a data controller, it is your responsibility to ensure the security and privacy of the personal data you process, by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Article 32 of the GDPR).

RÉPUBLIQUE FRANÇAISE

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

In the present case, given the sensitive nature of the information sent by unencrypted or weakly encrypted e-mail (i.e. names, first names, addresses, account numbers and amounts deposited), illegitimate access to these data by malicious third parties may entail a risk for the data subjects (in particular, attempts at extortion from third parties who may know the address and amount deposited at the time of the opening of the term account). Therefore, it appears necessary to communicate these data via a secure communication channel.

Yet, following the first exchange between the CNIL and your services, the security flaw reported by the complainants was confirmed. Corrective measures were taken to remedy this situation by increasing the level of security in the processing of the personal data of customers with fixed-term deposit accounts.

However, these first corrective measures (isolation of personal data in a separate document protected by a password) did not provide adequate protection insofar as the encryption of documents containing clients' personal data was too weak and thus made documents easily accessible by a third party.

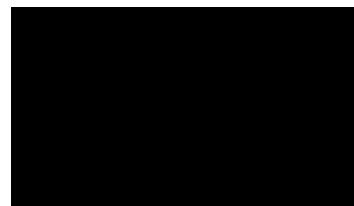
Nevertheless, I note that this problem has since been corrected: the email acknowledging receipt of the subscription documents no longer contains any personal data. Subsequent communications containing personal data of your customers are now sent by post.

I also take note of the establishment of a customer area (Online Banking) effective since October 20, 2020 allowing secure access to personal messaging (without storage of documentation).

I therefore note that [REDACTED] has brought the processing of the personal data of its customers implicated by these three complaints into conformity by taking the appropriate technical and organisational measures to remedy the security and confidentiality defects identified.

Finally, I would like to point out that this decision, which closes the examination of the aforementioned complaints, does not preclude the CNIL from using, in the event of new complaints, all the other powers conferred to it under the law of January 6th, 1978 as amended and the GDPR.

Yours sincerely,



Copy to [REDACTED] Data Protection Officer

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

The President



Letter with acknowledgment of receipt

No.: 2C 156 060 5291 9

Examination of the case:

Paris, on November 22th, 2021

No./Ref.: [REDACTED] RAL211050

Complaint no. 20006778

(to be referenced in all correspondence)

Mr. President,

This is further to the exchanges that took place between the CNIL's complaints department and the data protection officer of the [REDACTED] company in the context of the examination of [REDACTED]; complaint, which had been transmitted to us by the Italian data protection authority pursuant to the cooperation procedures between European authorities (Articles 56.1 and seq. of the General Data Protection Regulation « GDPR »).

[REDACTED] had lodged this complaint against [REDACTED] after receiving on May 9th, 2019 an e-mail from [REDACTED] showing the e-mail addresses of its 25 recipients.

First of all, I remind you that it belongs to the data controller to implement appropriate technical and organisational measures to ensure a level of security of personal data appropriate to the risk for the rights and freedoms of data subjects (Article 32 GDPR).

Concerning the personal data breach itself, the investigations led internally within your company reveal that « *an update of the library used for the [REDACTED] platform has led to some bugs, including one affecting personal data* ».

I note that this incident has been resolved by your technical teams in few hours and that measures have been taken in order to prevent such incident from occurring again.

It appears indeed that some measures compliant with customs and state of the art, such as carrying out tests after each modification of the platform's source code or updating library for instance, could have prevented such an anomaly. I take note in this regard that tests covering the code which manages the sending of emails, such as the one at stake, have been reinforced since then and include now a specific check on the risk of disseminating the addresses of other recipients.

RÉPUBLIQUE FRANÇAISE

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

Secondly, I note that the [REDACTED] company has notified to the Commission this data breach (notification no. FR2 [REDACTED]) upon receipt of the letter addressed to it.

I remind you that each data controller has to notify the personal data breach to the supervisory authority competent without undue delay « and, where feasible, not later than 72 hours after having become aware of it » (Article 33.1 GDPR). Where this notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

In this regard, I point out that your company has indicated that it has focused on fixing the incident and wrongly considered not being required to notify such violation « *because of the low sensitivity of the concerned data (professional e-mail addresses)* ».

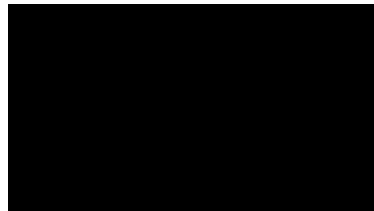
Yet, as underlined by your services, the notification duty does not depend on the nature of the data at stake but whether or not there is a risk for their privacy, risk that did exist in this particular case in view of the disclosure concerned. I further observe that it stems from this notification that around 2000 individuals would in fact be concerned by such breach.

I take note however of the commitment taken by your company, for the future, to make sure to notify such type of incident to the CNIL, without undue delay. I note that an internal memo reminding the process to follow in case of data breach has now been issued to all [REDACTED] services.

The explanations brought, the isolated nature of this incident as well as the measures rapidly taken by your services further to the Commission's intervention lead me, in agreement with other European data protection authorities concerned by the processing of data of individuals that have registered on the website [REDACTED] to issue reprimands to the [REDACTED] company on its obligations of security and notification provided under Articles 32 and 33 GDPR, in accordance with the provisions of Article 58.2.b) of the GDPR.

I specify that this decision, which closes [REDACTED], complaint, does not preclude the CNIL from using, notably in case of new complaints, all its other powers that are granted by the GDPR and by the French law of January 6th, 1978 as amended.

Yours Sincerely,



This decision may be appealed to the French Council of State within two months of its notification.

The Chair



Registered letter with acknowledgement of receipt

AR No: [REDACTED]

Investigation of the case:

Paris, on November 29th, 2021

Ref. No.: [REDACTED] 213278

Referral no. 20019846
(to be quoted in all correspondence)

Dear Chair,

I am following up on the complaint from [REDACTED] which was forwarded to the Commission Nationale de l'Informatique et des Libertés (CNIL – French Data Protection Authority) by the Dutch personal data protection authority (Autoriteit Persoonsgegevens) in accordance with the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] filed a complaint with his national data protection authority against [REDACTED], a brand belonging to the [REDACTED] company established in France. He reports difficulties encountered in exercising his right to object to receiving electronic marketing. Indeed, the complainant indicates that having attempted on several occasions to do so, in particular by sending two emails on April 7 and May 23, 2019, he continued to receive marketing emails.

The exchanges that have taken place between CNIL services and the Data Protection Officer (DPO) of [REDACTED] as part of the investigation of this complaint, the following elements emerge.

On the basis of the research carried out by your services, it was indicated that the complainant's request to object to the reception of direct marketing was taken into account by your services on March 24, 2019 and that the latter received no marketing e-mail as of that date except for an email on April 7, 2019 and a message wishing him a "Happy birthday" sent on [REDACTED]

In this regard, your DPO specifies that the "Happy birthday" email was not categorized as constituting a marketing message by the teams but that this has since been corrected.

RÉPUBLIQUE FRANÇAISE

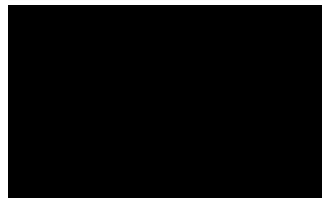
3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Regarding the email of April 7, 2019, your DPO clarified that it was difficult to determine the reasons for sending the latter, several months later, but that it was likely that this was due to the poor synchronization that existed in 2019 between the database containing user opt-in / opt-out information and the CRM (customer relationship management) tool. I note that the teams have since carried out a complete overhaul of the replication system between the database and the CRM tool in order to secure this synchronization and prevent such mailings from happening again.

The explanations provided and the measures already taken to avoid repeating the facts that are the subject of this complaint have led me, in agreement with the other European data protection authorities, **to close it**.

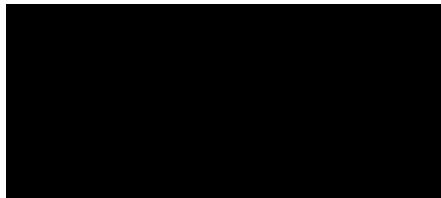
However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,



Copy to [REDACTED] Data Protection Officer

The Chair



Paris, on December 6, 2021

Ref. No. : [REDACTED] RAL211026

Referral no. 20019819

(to be quoted in all correspondence)

Dear Director,

I am following up on the various exchanges that have taken place between the departments of the *Commission Nationale de l'Informatique et des Libertés* ("CNIL" - French Data Protection Authority) and the Data Protection Officer of [REDACTED] as part of the investigation of [REDACTED]'s complaint, transmitted to the CNIL by the Hungarian Data Protection Authority pursuant to Article 56.1 of the General Data Protection Regulation ("GDPR").

[REDACTED] had lodged a complaint with his national data protection authority against [REDACTED] a subsidiary of [REDACTED] concerning the difficulties encountered in accessing information concerning the processing of personal data relating to the product recall procedure.

On receipt of this complaint, the Hungarian Data Protection Authority asked [REDACTED] for information. The latter's counsel stated that [REDACTED] was data controller concerning the processing of personal data relating to product recall, which was confirmed by [REDACTED]'s data protection officer and led the CNIL to take up the investigation of this referral.

The failures noted at the time of the exchanges between the CNIL and [REDACTED] lead me, in agreement with the other European data protection authorities concerned by the processing implemented, to remind [REDACTED] of its obligations, in accordance with the provisions of article 58.2.b) of the GDPR.

In the present case, [REDACTED] indicated that when he went to the cash register of the [REDACTED] store, located at [REDACTED] to purchase a product, he was asked to enter his email address in order to be notified in case of a product recall. The complainant then stated that he wanted to have the assurance that the personal data collected would be used only for the recall of the product.

RÉPUBLIQUE FRANÇAISE

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

The store's customer service is said to have refused to provide such a guarantee and suggested that he refer to the privacy policy available on [REDACTED] website, [REDACTED]

However, although information on the processing of personal data concerning product recall was present on the [REDACTED] website, it did not appear on the decathlon [REDACTED] website.

On this point, I remind you that in accordance with Articles 12 and 13 of the GDPR, the data controller is required to provide data subjects with certain information on the processing of personal data concerning them in a concise, transparent, understandable and easily accessible manner, in clear and simple terms.

In this case, the privacy policy stated on the website [REDACTED] did not mention the existence of the processing of personal data relating to product recall, which constitutes a breach of Articles 12 and 13 of the GDPR.

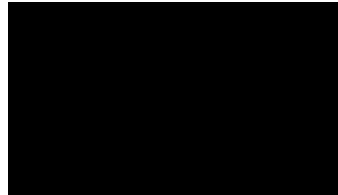
Nevertheless, I note the changes made to the information notices on the website [REDACTED] following the intervention of the CNIL departments with the DPO of [REDACTED]. Indeed, the privacy policy entitled '[REDACTED]' now contains information on the processing of personal data relating to product recall.

A note has also been added at the bottom of the home page of the website [REDACTED], entitled [REDACTED] dedicated specifically to the processing of personal data relating to product recall.

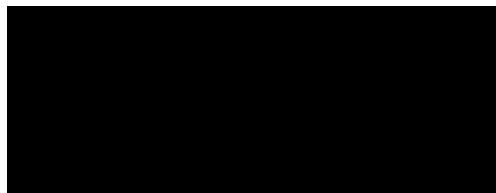
Finally, I note that the processing of this case has led to the other [REDACTED] subsidiaries within the European Union also being alerted so that "*the same level of information is accessible by all customers of the brand*".

I would like to point out that this decision, which closes the investigation of [REDACTED]'s complaint, does not preclude the CNIL from making use, particularly in the event of new complaints, of all the other powers attributed to it by the GDPR and by the amended Act of 6 January 1978.

Yours faithfully,



The President



LRAR n° 2C 137 386 0347 4

Examination of the case:

Paris, on December 22nd, 2021

No./Réf.: [REDACTED] CM214287

Case no. 21004812
(To be referenced in all correspondence)

Dear Mr. President,

This is further to the exchanges that took place between the services of the French data protection authority (Commission nationale de l'informatique et des libertés "CNIL") and the data protection officer of [REDACTED] company within the framework of the examination of [REDACTED]'s complaint, transmitted to the CNIL by the German data protection authority from Bavaria pursuant to Article 56.1 of the General Data Protection Regulation ("GDPR").

This complaint was about the security and confidentiality of booking confirmation emails sent by the [REDACTED]. Indeed, [REDACTED] stated that he had booked a hotel room in [REDACTED]. The emails confirmation of his reservation received in this respect from [REDACTED] on December 3rd, 7th and 8th, 2019 were passing through the server [REDACTED] which was not using TLS protocol.

First, in response to our electronic mail of April 1st, 2021, your company specifies that the mail server [REDACTED] is managed by the [REDACTED] company to which [REDACTED] has entrusted services relating notably to the sending of electronic booking confirmations. This server benefited from the standard settings recommended by your provider [REDACTED]. Thus, it stems from your response that the TLS setting was indeed activated for the most common recipient mail servers (google, yahoo, icloud...). However, for other less common recipient servers (such as the [REDACTED] server used by the complainant), this setting was not activated.

On this issue, your company argues that the systematic activation of the TLS protocol for mail servers would be a practice mainly known in the banking sector. It would indeed be "*likely to affect the performance of emails reception, which can be critical in the case of booking confirmations which, in addition to being required by the regulations, are very much expected by customers who want to be reassured that their purchase is going well*". Your company adds that the absence of activation of the TLS protocol would imply attack capabilities that are not available to "mainstream" hackers and that "*if successful, the sole concerned data would be those contained in the booking confirmation, which are not of a sensitive nature*".

REPUBLIQUE FRANÇAISE

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

Yet, it belongs to the processor to implement “*appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate (...) encryption of personal data*” (Article 32.1.a GDPR).

In this case, the sender is more precisely required to ensure an end-to-end encrypted transport channel at “*the state of the art*”, and this, for an end-to-end management of its electronic shipments. He must therefore guarantee an encrypted transport channel between its sending server (████████) and all recipients servers, such as the one here (████). Indeed, the transmission of personal data through public networks shall be subject to security measures enabling to ensure its confidentiality and integrity. Therefore, the implementation of a protocol, such as the TLS protocol, enabling the encryption and authentication of data appears necessary in such context.

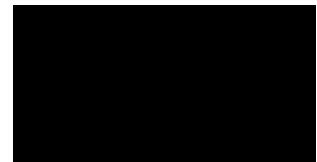
Therefore, by not providing an encrypted transport channel when sending the booking confirmation which included █████'s personal data, █████ has failed to comply with its security and confidentiality obligations provided under Article 32.1 of the GDPR.

However, I note that your company has of its own doing activated the TLS protocol on April 23rd, 2021 systematically in order to test the possible impact on performance. After a monitoring period, in the absence of regressions compared to the previous configuration, your company decided to keep this setting for sending its electronic communications. All sendings from the █████ server are now carried out with the activated TLS protocol (screenshot provided in support).

In this respect, I would like to remind you that in order to guarantee in an optimal way the security of exchanged data, the TLS protocol must be associated with cryptographic chains that have no known vulnerabilities. That is why its version 1.3, which only offers state-of-the-art cryptographic algorithms, should be privileged. For all intents and purposes, the French Agency for the Security of Information Systems (ANSSI) has published several security recommendations for the TLS protocol in its note version 1.2 of 03/26/2020, available at the following URL : <https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/>.

The answers provided by your company, and in particular the measures taken by the latter, lead me, in agreement with other European data protection authorities concerned by the processing, **to proceed to the closure of this complaint**.

Yours Sincerely,



Summary Final Decision Art 60

Investigation

Administrative fine

EDPBI:FR:OSS:D:2021:310

Background information

Date of final decision:	30/12/2021
Date of broadcast:	05/01/2022
LSA:	FR
CSAs:	DE (BW, BY, BE, NI), ES, BE, IT, LU, NL
Legal Reference:	Article 5, Article 13, Article 17, Article 28 and Article 32.
Decision:	Administrative Fine
Key words:	Cooperation with the supervisory authority, Data retention, Data security, Data subject rights, Password, Personal data breach, Right to be informed, Right to erasure

Summary of the Decision

Origin of the case

The controller's is a company selling furniture online and in store. It has its main establishment in France. On 24 April 2019, 9 May 2019 and 5 June 2019 the LSA's team carried out an online investigation into the processing accessible from the company's domain and an on-site investigation. The purpose of these investigations was to verify the company's compliance with the GDPR and the national data protection law. The online investigations conducted by the LSA focused on the manner in which personal data for customers and prospective customers had been processed by the company.

In accordance with Article 56 GDPR, on 1 July 2020, the LSA informed all the European supervisory authorities of its competence to act as lead supervisory authority. In October 2020, the LSA submitted a draft order to the CSAs. The Berlin SA raised a relevant and reasoned objection within the meaning of Article 60(4) GDPR, requesting that the draft order be turned into a draft penalty, and more specifically an administrative fine. In support of this

request, the CSA pointed out the high number of data subjects concerned and the duration of the violations. The LSA then shared a revised draft decision, to which no CSA objected.

In its defence, the controller has contested the Berlin SA's objections and expressed its surprise at the importance given to them, bearing in mind the low percentage of the controller's sales in Germany. The company considers that it should have been the subject of an order, as initially proposed by the LSA, and not to a penalty.

Findings

Regarding the proceedings, the LSA recalled that the BE SA's objections had been expressed within the framework of the cooperation and consistency mechanism provided for under Chapter VII GDPR, which intends to ensure harmonisation of the SA's enforcement policy. Regarding the controller's obligations under Article 5(1)(e) GDPR, the LSA established a breach of this provision, in so far as the controller had not defined and implemented any satisfactory retention period policy on the date of the investigation.

Regarding the obligation under Article 13 GDPR to provide the data subjects concerned with information relating to the processing of their personal data, the LSA found that the information was not complete. In this context, the LSA pointed out that the link between the controller's failure to implement data retention period and the lack of information for individuals did not prevent these two breaches from existing as such.

Furthermore, the LSA established a breach of the obligation to comply with requests to delete personal data pursuant to Article 17 GDPR, because there were cases in which the controller had simply deactivated the customer's account without actually deleting the personal data. In addition, the controller's relationship with one of its processors had not been governed by any legal act, in breach of Article 28 GDPR.

Finally, the LSA also held that the controller had failed to ensure the security of personal data pursuant to Article 32 GDPR.

Decision

The LSA noted that, as part of the penalty proceedings, the controller has demonstrated having taken measures to ensure compliance with the GDPR. Nevertheless, the LSA held that this could not exempt the company from its responsibility for the past and imposed an administrative fine of EUR 120,000 in respect of the breaches of Articles 5(1)(e), 13, 17, 28 and 32 GDPR.

Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:FR:OSS:D:2021:313

Background information

Date of final decision:	28 December 2021
Date of broadcast:	11 January 2022
LSA:	FR
CSAs:	DEBW, DEBY, DEBE, DEHB, DEHH, DEHE, DEHI, DEMV, DENW, DERP, DESL, DESN, DEST, DESH, DESH, DETH, IT, NL, ES
Legal Reference(s):	Article 28 (Processor), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority), Article 34 (Communication of a personal data breach to the data subject)
Decision:	Administrative fine
Key words:	Clients, Personal data breach, Data security, Publicly available data, Finance

Summary of the Decision

Origin of the case

The controller is a payment service provider offering to its customers (merchants) solutions for managing recurring payments in SEPA. In order to provide these services, it processes personal data of its customers' debtors. In 2015, the controller carried out a research project on anti-fraud mechanism, for which it imported personal data of its clients' debtors on a dedicated server. Yet, the server was not subject to any special security procedures and the personal data remained freely accessible via a specific URL until 2020, when the breach was reported to the controller by one of its customers. Following this, the controller immediately took corrective measures and notified the LSA of the breach. The data of more than 12 million debtors was affected. It consisted of surname, first name, title, e-mail address, post address, telephone number, BIC/IBAN information.

Findings

The LSA carried out an investigation and received additional information from the company. It was established that the latter had acted as data processor hiring sub-processors for the processing carried out in the context of the services provided to merchants, and as data controller with regard to the research project resulting in the data breach. The LSA characterised a number of breaches. First, the company had failed to provide a formal legal framework for the processing carried out by the sub-processors and had merely sent them a questionnaire with no binding force. Furthermore, some of the contracts with its processors did not satisfy the requirements of Art. 28(3) and (4) GDPR. Second, the company had not ensured security of personal data within the meaning of Art. 32 GDPR. The continuous breach consisting of leaving personal data freely accessible online could not be explained by isolated human negligence, since security deficiencies were the result of repeated insufficiency and the controller should have ensured the security of the data in question at several stages. In addition, the LSA took the view that the lack of evidence of fraudulent use of the data did not affect the characterisation of the breach of the security obligation. Finally, the LSA also established a breach of the controller's obligation to notify data subjects of a personal data breach pursuant to Art. 34 GDPR. According to the LSA, given the nature of the personal data, the volume of data subjects, the ease of identifying the persons affected by the breach and the possible consequences for the data subjects, the risk associated with the breach could be considered high and communication to the data subjects should have been made.

Decision

In light of the above, the LSA decided to impose on the controller an administrative fine of EUR 180.000 for the infringement of Articles 28(3), 28(4), 32 and 34 GDPR and publish the decision, which will no longer identify the company at the end of a period of two years following its publication.

The President



Paris, on February 3, 2022

Letter with acknowledgment of receipt

No:

To be quoted in all correspondence:

Ref. No.: [REDACTED] MDM2 [REDACTED]

Formal notice no. MED 2022-003 of February 3, 2022

Case no. [REDACTED]

Dear Sir or Madam,

I am following up on the complaint from [REDACTED] which was forwarded to the French data protection authority (CNIL) by the data protection authority in Luxembourg ("the Commission nationale pour la protection des données du Grand-Duché de Luxembourg (CNPD)") pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] lodged a complaint with his data protection authority against the company [REDACTED] publisher of the website [REDACTED] established in France, concerning the difficulties encountered in the exercise of his rights of erasure and objection. In this case, the complainant requested the deletion of his personal data linked to his e-mail addresses « [REDACTED] » and « [REDACTED] » by a first e-mail of 27 May 2020 sent to the contact address « [REDACTED] » then by a follow-up email sent on 11 June 2020.

The elements communicated to the Commission in the email dated 10 February 2021 in the context of the investigation of this complaint give rise to the following observations.

Firstly, [REDACTED] indicated to my services that he had tried to unsubscribe from marketing emails using the link at the bottom of them, without success.

It was indicated that this link works in principle, that it is managed manually and that the possible failure to act on the complainant's request might result from the disorganisation of your services due to the health crisis.

Secondly, it was specified that only the e-mail address [REDACTED] was registered in [REDACTED] s customer databases. It was then indicated that the complainant's request generated an acknowledgment of receipt from the IT department on 15 June 2020 and that his email address was actually deleted on the following 16 June but that the IT department, which acknowledged receipt of the complainant's request, supposedly "*inadvertently forgot to confirm to him that it had done what was necessary*". However, it was brought to our attention that the complainant is said to have received a marketing email on 29 July 2020 sent through " [REDACTED]" (*copy attached*). The Commission nationale pour la protection des données du Grand-Duché de Luxembourg also informed us that the complainant then would have received a marketing email in October 2020.

RÉPUBLIQUE FRANÇAISE

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

Yet, I remind you that any individual can request at any time the erasure of personal data concerning them (articles 17 and 21.1 of the GDPR).

Thus, it appears that the complainant's personal data would not have been suppressed from the [REDACTED]'s files on 16 July of 2020 as it was mentioned in the letter of 10 February received by the Commission.

Then, when my services tried to reach your services using the contact email address "[REDACTED]", which was indicated on your website as being the address for exercising the rights of data subjects, they received the response below (*screenshot*).



Translation of the screenshot: "*Wednesday 13/01/2021 15:35, [REDACTED], Auto: Complaint n° [REDACTED] to [REDACTED]*. We cannot respond favorably to your request. Please write to your restaurant by visiting our website [REDACTED] section "Contact us", choosing "Contact your restaurant", or contact your restaurant by phone."

I am surprised by the answer of your services dated February 10, 2021 in which it was indicated that "*the automatic response message generated by the address '[REDACTED]' indicates, in fact, not "we cannot respond favorably to your request" as stated in [our] letter, but the following: "Hello, This address is not dedicated to receiving messages. If you wish to write to your restaurant, we invite you to go to the "Contact us" section, [REDACTED] of our website. Then choose "Contact your restaurant" and select the city of your restaurant or do not hesitate to contact your restaurant directly by phone. [...]"*

I remind you that you must facilitate the exercise of the rights of data subjects (article 12.2 of the GDPR).

Thus, referring people to the "Contact us" form on the website, while they are exercising their rights via the contact email address made available to them for this purpose, does not facilitate the exercise of the rights of the data subjects.

Thenceforth, you have to set up an intelligible system to facilitate the exercise **of all rights** available to data subjects under the GDPR.

In addition, you must "*provide the data subject with information on the measures taken following a request made in accordance with Articles 15 to 22, as soon as possible and in any event within one month from receipt of the request*", this period may be extended by two months due to the complexity and number of requests, and on condition that the data subjects are informed of this extension and the reasons for the postponement (article 12.3 of the GDPR).

Thus, you shall inform all applicants that their request for erasure has been taken into account within one month, or in the event of difficulties caused by the complexity or number of requests, within two months provided that you informed the applicant about this extension and the reasons for this postponement.

Consequently, pursuant to Article 20 of the French law no. 78-17 of January 6, 1978 as amended and to Article 58.2.c of the general data protection regulation, and in agreement with other data protection authorities concerned by the processing, the company [REDACTED] located at [REDACTED], is hereby given order to comply, within twenty (20) days from notification of this decision and subject to measures that it may already have adopted, to:

- proceed to the erasure of all personal data concerning [REDACTED];
- inform [REDACTED] that his erasure and opposition requests have been taken into account;
- take the necessary measures to set up an intelligible system to facilitate the exercise of all rights available to data subjects under the GDPR;
- justify to the CNIL that these requests have been complied with, within the time limit set.

After this time-limit, if the company [REDACTED] has complied with this order to comply, I will address it a letter for informing it that this formal notice procedure is closed.

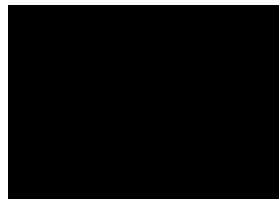
On the contrary, if the company [REDACTED] has not complied with this order to comply, I could seize CNIL4S Restricted Committee in order for one or several of the measures set out under Article 20 and subsequent of French law of January 6th, 1978 as amended to be pronounced.

I also draw your attention to the retention period of the personal data for which you indicate that you do not keep personal data of your prospective customers after a period of 36 months following the last contact. However, the complainant indicated that his last purchase from your service was 4-5 years ago. This last contact dates back more than 36 months. In this respect, we recall that the GDPR (Article 5.1 e) specifies that personal data must be "*kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed*".

The Commission's services ([REDACTED]), legal officer in the rights and complaint department - [REDACTED] are at your disposal for any further information.

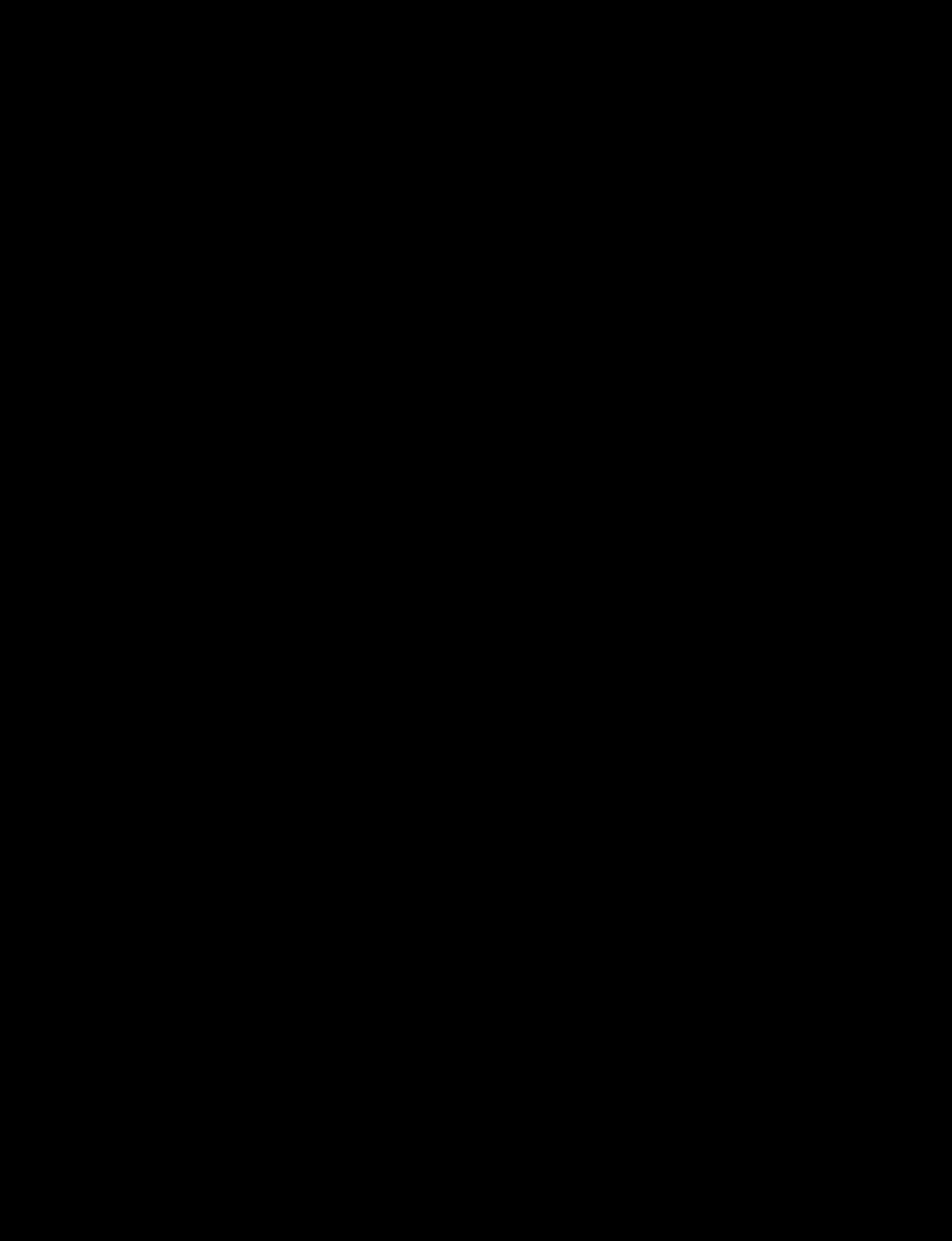
This decision may be appealed before the French State Council within two months a period of following its notification.

Yours sincerely,



De:
Envoyé:
À:
Objet:

[REDACTED]
mercredi 29 juillet 2020 14:00
[REDACTED]
[REDACTED]



**Decision [REDACTED] ordering the company
to comply**

(No. [REDACTED])

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-256C of 12 October 2020 of the Chair of the CNIL instructing the General Secretary to carry out, or have carried out, an audit of the data processing activities accessible from the domain '[REDACTED]' or concerning personal data collected from this domain;

Having regard to referral No. [REDACTED];

Having regard to the other exhibits;

I. The procedure

[REDACTED] (hereinafter "the company" or "[REDACTED"]"), whose registered office is [REDACTED], was established in [REDACTED] to perform a distance selling activity.

On 19 August 2020, the Commission nationale de l'informatique et des libertés (French data protection authority, hereinafter "CNIL") received a complaint (no. [REDACTED]) relating to the transfer of personal data of the complainant (represented by [REDACTED]), to the United States of America, collected during his visit to the website [REDACTED]. [REDACTED] has filed 101 complaints in the 27 Member States of the European Union and the three other members of the European Economic Area (EEA) against 101 data controllers alleged to transfer personal data to the United States.

Pursuant to decision [REDACTED] of the CNIL Chair dated [REDACTED], a CNIL delegation carried out a documentary audit by sending a questionnaire to [REDACTED] on [REDACTED] and a request for further information on [REDACTED]. The company replied in letters [REDACTED].

The questionnaires concerned the transfer of data of visitors to the French language version of the website [REDACTED], which uses the Google Analytics service.

[REDACTED], the company informed the CNIL that it had decided to integrate the Google Analytics functionality on its website [REDACTED] and that the statistics obtained via Google Analytics concerned individuals in several member states of the European Union. The processing activity resulting from the integration of the Google Analytics functionality on its website therefore appears to meet the definition of cross-border processing within the meaning of Article 4.23.b) of the GDPR.

[REDACTED]

Pursuant to Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "GDPR" or the "Regulation"), [REDACTED], the CNIL informed all European supervisory authorities of its competence to act as lead authority regarding the cross-border processing implemented by the company, this competence deriving from the fact that the company's principal place of business is located in France.

Within the meaning of Article 4, point 22 of the GDPR, [REDACTED] data protection authorities are concerned, namely the authorities [REDACTED]

[REDACTED]

On 4 January 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

This draft decision did not give rise to any relevant and reasoned objections.

II. On the data processing in question and the responsibility for processing

The responses [REDACTED] sent to the audit delegation revealed that the company integrated the Google Analytics feature on the website [REDACTED] for the purpose of measuring its audience and the performance of the company's media campaigns. The company stated that Google Analytics notably enabled the tracking of an individual if the user had not refused such use. Indeed, by combining a user's unique identifier with that user's data from one or more sessions initiated from one or more devices, Google Analytics is able to obtain more accurate details of users (by identifying a user as an individual user, even in a different session).

[REDACTED]

[REDACTED]

Google Analytics works by including a piece of JavaScript code on the pages of a website. When a user visits a webpage, this code triggers the uploading of a JavaScript file and then

performs the tracking operation for Google Analytics. The tracking operation consists of recovering data relating to the query through various means and sending this information to the Google Analytics servers.

Website managers who integrate the Google Analytics service may send instructions to Google for the processing of data collected through Google Analytics. These instructions are transmitted through the tag manager that manages the tracking code they have integrated into their website and through the tag manager settings. The website manager can apply different settings, for example, regarding the data retention period. The Google Analytics feature also allows website managers to monitor and maintain the stability of their website, for example by keeping them informed of certain events such as a peak in audience or the fact that there is no traffic at all. Google Analytics also allows website managers to measure and optimise the effectiveness of advertising campaigns conducted using other Google tools.

In this context, Google Analytics collects the user's http query and information about the user's browser and operating system, among other things. [REDACTED] an http request, for any page, contains details of the browser and the device making the query, such as the domain name and browser information such as its type, referer, and language. Google Analytics stores and reads cookies on the user's browser to evaluate the user's session and other information on the query.

When this information is collected, it is transmitted to the Google Analytics servers. [REDACTED] [REDACTED] all data collected through Google Analytics are hosted in the United States.

Thus, data collected on the [REDACTED] website via Google Analytics are transferred to the United States.

As regards these transfers, it appears from the exhibits that the contract [REDACTED] [REDACTED] concerning the Google Analytics feature refers to an appendix entitled Google Ads Data Processing Terms. This appendix contains standard contractual clauses governing the transfer of personal data to the United States of America under the Google Analytics service. The company indicated that it had no evidence in its possession to consider that these clauses had not been complied with.

[REDACTED] it has implemented additional legal, organisational and technical measures to regulate data transfers under the Google Analytics service.

All of these elements show that, by deciding to implement the Google Analytics feature on this website for evaluation and optimisation purposes, the company managing the website [REDACTED] determined the means and purposes of the collection and processing of the data obtained further to the integration of Google Analytics on its website and should be considered the data controller within the meaning of Article 4.7 of the GDPR.

III. On the qualification of personal data

It can be established that the data collected under the Google Analytics feature and transferred to the United States of America constitute personal data.

Article 4.1 of the GDPR defines personal data as "*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."

It should be noted that online identifiers, such as IP addresses or information stored in cookies can commonly be used to identify a user, particularly when combined with other similar types of information. This is illustrated by Recital 30 GDPR, according to which the assignment of online identifiers such as IP addresses and cookie identifiers to natural persons or their devices may "*leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*" In the particular case where the controller would claim to not have the ability to identify the user through the use (alone or combined with other data points) of such identifiers, he would be expected to disclose the specific means deployed to ensure the anonymity of the collected identifiers. Without such details, they cannot be considered anonymous.

Therefore, it is necessary to examine to what extent the implementation of Google Analytics on a website allows the website manager and [REDACTED] to render a data subject (a visitor of the website in question) identifiable.

In its reply, [REDACTED] states that the following categories of personal data are processed under the Google Analytics feature:

- a visitor's identifier (the identifier of the Google Analytics visitor cookie, i.e. the Google Analytics customer ID);
- for visitors who have logged into the website through a user account, an internal [REDACTED] identifier;
- the order identifiers, if any;
- IP addresses.

The company asserts that IP addresses are '*anonymised*', without specifying what process is used to make these addresses anonymous. However, the company describes these data as personal data.

With regard to visitor identifiers, it should be noted that these are unique identifiers intended to differentiate individuals. In the present case, these identifiers may also be combined with other information, such as the address of the website visited, metadata relating to the browser and operating system, the time and data relating to the visit to the website, and the IP address. This combination of information further differentiates individuals.

For this reason, when several elements are combined, they can make it possible to individually identify visitors to the [REDACTED] website, on which Google Analytics is implemented. It is not required to know the actual visitor's name or (physical) address since, in accordance with recital 26 of the GDPR, such singling out of individuals is sufficient to make the visitor identifiable.

Should it be decided otherwise, the scope of the right to data protection, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, would be undermined as it would allow companies to specifically single out individuals along with personal information (such as when they visit a specific website) while denying them any right of protection against such singling out. Such a restrictive view that would undermine the level of protection of

individuals is also not line with the case law of the Court of Justice of the European Union, which repeatedly ruled that the scope of the GDPR has to be understood in a very wide manner (see, for example, C-439/19, paragraph 61).

The CNIL further notes that for users of the [REDACTED] website who have identified themselves through a user account, or those who have placed an order, the data can be directly connected with identifying data.

Moreover, [REDACTED] in the context of using Google Analytics, and under some Google account settings, Google is informed that a user connected to a Google account has visited a particular website. Personal data relating to this account are therefore collected.

As a result, it must be considered that the data in question should be regarded as personal data within the meaning of Article 4 of the GDPR.

IV. On the breach of the obligation to regulate transfers of personal data outside the European Union

Article 44 of the GDPR states: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

Chapter V of the Regulation provides for various tools to ensure a level of protection substantially equivalent to that guaranteed within the European Union, pursuant to Article 44 of the Regulation:

- adequacy decisions (Article 45);
- appropriate safeguards (Article 46);

In the absence of an equivalent level of protection, it establishes derogations for specific situations (Article 49).

In the present case, it must be verified whether the export of personal data to the United States of America comply with Article 44 GDPR and, in particular, whether the export was based on one of these grounds, and if it was, if the relevant measures were taken.

4.1 Adequacy decisions

In its judgement of 16 July 2020 (C-311/18), the Court of Justice of the European Union invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the European Union-US Privacy Shield, without maintaining its effects.

In the absence of another relevant adequacy decision, the transfers in question may not be based on Article 45 of the GDPR.

4.2 Appropriate safeguards

Article 46.1 of the Regulation provides that "*In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*"

Article 46.2 of the Regulation provides that "*The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: [...] (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).*"

4.2.1 Standard data protection clauses

In the present case, the company and Google have entered into standard contractual clauses for the transfer of personal data to the United States (Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors). These clauses are in line with those published by the European Commission in Decision 2010/87/EU.

In this context, it must be emphasised that standard contractual clauses are a transfer tool within the meaning of Chapter V of the Regulation and were not challenged as such by the Court of Justice in its judgement of 16 July 2020 (C-311/18). However, the Court considered that it stemmed from the contractual nature of these clauses that they could not be binding on the authorities of third countries. In particular, 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*" (C-311/18, point 126, emphasis added).

A further analysis of the legal situation of the USA is not required though, as the CJEU has already provided such analysis in its aforementioned judgement. Indeed, the Court found that the surveillance programmes in question do not correlate to the minimum safeguards arising from the principle of proportionality under Union law, such that the surveillance programmes based on these provisions cannot be regarded as limited to what is strictly necessary (point 184). Moreover, the Court found that the legal framework in question did not confer on data subjects rights actionable in the courts against the US authorities, from which it follows that these persons have no right to an effective remedy (point 192).

The analysis of the CJEU is relevant in the present case, since Google LLC (as importer of the data to the USA) is to be qualified as a provider of electronic communications services within the meaning of 50 US. Code § 1881(b)(4) and is therefore subject to surveillance by US. intelligence services in accordance with 50 US. Code § 1881a ("FISA 702"). Google LLC

therefore has the obligation to provide the US government with personal data when requested FISA 702.

As can be seen in the Google Transparency Report, Google LLC is regular subject to such access requests by US. intelligence services.

Considering the fact that the Court of Justice declared the adequacy decision with the United States of America invalid due to the access possibilities of US intelligence services, and the fact that the conclusion of SCCs cannot by themselves ensure a level of protection as required by Article 44 GDPR as the guarantees they provide are left unapplied when such access requests are taking place. Indeed, the CJEU concluded the following: "*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*" (point 133).

4.2.2 Implementation of additional safeguards

In its recommendations 01/2020 of 18 June 2021, the European Data Protection Board (EDPB) has clarified that where the assessment of the law and/or practices in force of the third country may impinge on the effectiveness of the appropriate safeguards of the transfer tools the exporter is relying on, in the context of his specific transfer, which is the case here following the assessment by the CJEU, the exporter has to either suspend the transfer or implement adequate supplementary measures. The EDPB notes in this respect that "*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgement "Schrems II" if and to the extent that it – by itself or in combination with others - addresses the specific deficiencies identified in the assessment of the situation in the third country as regards its laws and practices applicable to the transfer*" (point 75).

Measures to supplement standard data protection clauses can be classified into three categories: contractual, organisational and technical (see point 47 of Recommendations 01/2020).

With regard to contractual measures, the EDPB noted that such measures: "*[...] may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country may provide [...]. 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 [...]*" (point 99, emphasis added).

As regards organisational measures, the EDPB highlighted that "*[...] Selecting 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" (point 128, emphasis added).

With regard to technical measures, the EDPB pointed out that "[...] These measures will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools and are, in particular, capable of impinging on the contractual guarantee of an essentially equivalent level of protection against access by the public authorities of that third country to that data" (point 77, emphasis added). It added that "The measures listed [in the guidelines] 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. 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" (point 79, emphasis added).

4.2.3 Supplementary measures implemented by Google

Google LLC, as the data recipient, has adopted contractual, organisational and technical measures to supplement the standard data protection clauses. [REDACTED]

Taking the considerations of the CJEU and the EDPB into account, it must now be verified whether or not the supplementary measures adopted by Google LLC are effective, meaning they address the specific issue of access possibilities of US intelligence services.

With regard to the *legal and organisational measures* adopted, it must be noted that neither the notification of users – should such notification even be permissible – nor the publication of a Transparency Report or a publicly available „policy on handling government requests” in fact prevent or reduce access possibilities of US intelligence services. Furthermore, it remains unclear how Google LLC’s „careful review of each request” on its permissibility is effective as supplementary measure, considering that according to the CJEU, permissible (legal) requests of US intelligence services are not in line with the requirements of the European Data Protection Law.

With regard to the *technical measures* adopted, it should be noted that it has not been clarified, either by Google LLC or by the company, how the measures described – such as the protection of communications between Google's services, the protection of data in transit between data centres, the protection of communications between users and websites, or “on-site security” – in fact prevent or reduce the possibilities of access by US intelligence services on the basis of the US legal framework.

As far as encryption technologies are concerned – such as for „data at rest” in data centres, as specifically mentioned by Google LLC as technical measure – it has to be noted that Google LLC as data importer nonetheless has an obligation to grant access or to turn over imported

personal data in their possession, including any cryptographic keys necessary to render the data intelligible (see Recommendations 01/2020, point 81). In other words: As long as Google LLC has the possibility to access the data of natural persons in clear text, such technical measure cannot be deemed effective in the present case.

As far as Google LLC brings forward that „(t)o the extent Google Analytics Data for measurement transferred by website owners is personal data, it would have to be regarded as pseudonymous”, it must be noted that universal unique identifiers (UUIDs) do not fall under the definition of Article 4.5 of the GDPR. While pseudonymisation may be a privacy-enhancing technique, the unique identifiers have, as already outlined above, the specific intention to single out users, not to act as safeguard. Apart from this, it has also been outlined above why the combination of unique identifiers with other elements (such as browser or device meta data and the IP-address) and the possibility to link such information to a Google Account in any case make an individual identifiable.

As far as Google LLC refers to an „Optional Technical Measure“ by means of an IP-Anonymization function, it must first be noted that such measure is – as the name indicates – optional and not applicable to all transfers. In addition, it is not clear from Google's response if this anonymisation takes place before the transfer or if the entire IP address is transmitted to the United States and only shortened after this transfer to the United States. Thus, from a technical point of view, there is potential access to the entire IP address before it is shortened.

Therefore, the supplementary measures adopted, as presented by Google, are not effective insofar as none of them addresses the specific issues in the present case, meaning none of them prevent access possibilities of US intelligence services or render these accesses ineffective.

4.3. The derogations provided for in Chapter V of the Regulation

Article 49 of the Regulation states "*1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:*

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; [...]”

The company argues that the transfer could be based on Art. 49.1.a of the GDPR by indicating that data subjects may refuse to allow Google to track their visit to the website.

However, users' consent to the storing of cookies during their visit to the website cannot be considered as equivalent to their having "*explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards*" within the meaning of Article 49.1.a of the Regulation. In this regard, it can be noted that the company, far from establishing

that such consent has been obtained, does not provide any information relating to these elements which would be provided to visitors of the website.

The company also invokes Article 49.1.b of the Regulation insofar as these functionalities are necessary for the proper functioning of the website and the detection of anomalies.

This argument is nevertheless not supported by any specific evidence and, above all, the company does not establish that there is a contractual relationship between it and all users of its website.

Consequently, the company cannot invoke Article 49 of the Regulation to justify the data transfers in question.

4.4. Conclusion

Therefore, it must be concluded that the company cannot invoke any of the tools provided for in Chapter V of the Regulation to justify the transfer of personal data of visitors to its website, and in particular unique identifiers, IP addresses, browser data and metadata, to Google LLC in the United States.

Accordingly, with this transfer of data, the company undermines the level of personal data protection of data subjects as guaranteed in Article 44 of the GDPR.

Consequently, [REDACTED] is hereby ordered to comply with the following, within one (1) month of notification of this decision, and subject to any measures it may have already implemented:

- bring the data processing activity under the Google Analytics service into compliance with Articles 44 et seq. of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, notably by ceasing processing activities which relate to the current version of the tool Google Analytics;
- provide supporting documentation to the CNIL confirming that the aforementioned request has been complied with within the time limit.

At the end of that period, if [REDACTED] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if [REDACTED] has not complied with this order notice by the end of that period, a rapporteur will be appointed to request the restricted committee to issue one of the penalties provided for by Article 20 of the French Data Protection Act of 6 January 1978, as amended.

The Chair

[REDACTED]

**Draft decision No. [REDACTED] ordering the company
[REDACTED] to comply**

(No. [REDACTED])

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-257C of 12 October 2020 of the Chair of the CNIL instructing the General Secretary to carry out, or have carried out, an audit of the data processing activities accessible from the domain [REDACTED] or concerning personal data collected from this domain;

Having regard to referral No. [REDACTED]

Having regard to the other exhibits;

I. The procedure

[REDACTED] (hereinafter "the company" or [REDACTED]), whose registered office is located at [REDACTED], is a retailer of sport articles in specialized stores.

On 19 August 2020, the Commission nationale de l'informatique et des libertés (French data protection authority, hereinafter "CNIL") received a complaint (no. 20013890) relating to the transfer of personal data of the complainant (represented by the association [REDACTED]), to the United States of America, collected during his visit to the website [REDACTED]. [REDACTED] has filed 101 complaints in the 27 Member States of the European Union and the three other members of the European Economic Area (EEA) against 101 data controllers alleged to transfer personal data to the United States.

Pursuant to decision No. 2020-257C of the CNIL Chair dated [REDACTED], a CNIL delegation carried out a documentary audit by sending a questionnaire to [REDACTED] on [REDACTED] and a request for further information on [REDACTED]. The company replied in letters [REDACTED]. The questionnaires concerned the

transfer of data of visitors to the French language version of the website [REDACTED], which uses the Google Analytics service.

[REDACTED] the company informed the CNIL that it had decided to integrate the Google Analytics functionality on its website [REDACTED] and that the statistics obtained via Google Analytics concerned individuals in several member states of the European Union. The processing activity resulting from the integration of the Google Analytics functionality on its website therefore appears to meet the definition of cross-border processing within the meaning of Article 4.23.b) of the GDPR.

[REDACTED]
[REDACTED]
[REDACTED].

Pursuant to Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "GDPR" or the "Regulation"), [REDACTED], the CNIL informed all European supervisory authorities of its competence to act as lead authority regarding the cross-border processing implemented by the company, this competence deriving from the fact that the company's principal place of business is located in France.

Within the meaning of Article 4, point 22 of the GDPR, [REDACTED] data protection authorities are concerned, namely the authorities of [REDACTED]

On 28 January 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

This draft decision did not give rise to any relevant and reasoned objections.

II. On the data processing in question and the responsibility for processing

The responses [REDACTED] sent to the audit delegation revealed that the company integrated the Google Analytics feature on the website [REDACTED]. This feature has been implemented for the purpose of measuring its audience (volume of traffic, number of unique visitors, origin of connection, type of terminal used, conversion rate of visitors into buyers, etc.); of analysing the path of visits in order to correct or improve the site; of understanding and having visibility on the display and ordering of products as well as their attractiveness; and finally of measuring and anticipating connection peaks.

[REDACTED]
[REDACTED]
[REDACTED]

Google Analytics works by including a piece of JavaScript code on the pages of a website. When a user visits a webpage, this code triggers the uploading of a JavaScript file and then performs the tracking operation for Google Analytics. The tracking operation consists of recovering data relating to the query through various means and sending this information to the Google Analytics servers.

Website managers who integrate the Google Analytics service may send instructions to Google for the processing of data collected through Google Analytics. These instructions are transmitted through the tag manager that manages the tracking code they have integrated into their website and through the tag manager settings. The website manager can apply different settings, for example, regarding the data retention period. The Google Analytics feature also allows website managers to monitor and maintain the stability of their website, for example by keeping them informed of certain events such as a peak in audience or the fact that there is no traffic at all. Google Analytics also allows website managers to measure and optimise the effectiveness of advertising campaigns conducted using other Google tools.

In this context, Google Analytics collects among other things the user's http query and information about the user's browser and operating system, among other things. [REDACTED] [REDACTED] an http request, for any page, contains details of the browser and the device making the query, such as the domain name and browser information such as its type, referer, and language. Google Analytics stores and reads cookies on the user's browser to evaluate the user's session and other information on the query.

When this information is collected, it is transmitted to the Google Analytics servers. [REDACTED] indicated that all data collected through Google Analytics are hosted in the United States.

Thus, data collected on the [REDACTED] website via Google Analytics are transferred to the United States.

As regards these transfers, it appears from the exhibits that the contract [REDACTED] concerning the Google Analytics feature refers to an appendix entitled Google Ads Data Processing Terms. This appendix contains standard contractual clauses governing the transfer of personal data to the United States of America under the Google Analytics service. The company indicated that it does not have any information that would enable to assess with certainty whether these clauses are respected.

[REDACTED] it has implemented additional legal, organisational and technical measures to regulate data transfers under the Google Analytics service.

All of these elements show that, by deciding to implement the Google Analytics feature on this website for evaluation and optimisation purposes, the company managing the website [REDACTED] determined the means and purposes of the collection and processing of the data obtained further to the integration of Google Analytics on its website and should be considered the data controller within the meaning of Article 4.7 of the GDPR.

III. On the qualification of personal data

It can be established that the data collected under the Google Analytics feature and transferred to the United States of America constitute personal data.

Article 4.1 of the GDPR defines personal data as "*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."

It should be noted that online identifiers, such as IP addresses or information stored in cookies can commonly be used to identify a user, particularly when combined with other similar types of information. This is illustrated by Recital 30 GDPR, according to which the assignment of online identifiers such as IP addresses and cookie identifiers to natural persons or their devices may "*leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*" In the particular case where the controller would claim to not have the ability to identify the user through the use (alone or combined with other data points) of such identifiers, he would be expected to disclose the specific means deployed to ensure the anonymity of the collected identifiers. Without such details, they cannot be considered anonymous.

Therefore, it is necessary to examine to what extent the implementation of Google Analytics on a website allows the website manager and [REDACTED] to render a data subject (a visitor of the website in question) identifiable.

The responses [REDACTED] revealed that the following categories of data are processed under the Google Analytics feature:

- data relating to orders placed, which are not directly identifying;
- an identifier of the visitor cookie Google Analytics;
- the visitor's IP address.

The company explains that it changes the identifiers of the Google Analytics cookies by randomly determining a new identifier. It also specifies that the last bytes of IP addresses are removed.

With regard to visitor identifiers, it should be noted that these are unique identifiers intended to differentiate individuals and thus identify them by allowing the players in question to be able to "recognize" them later. The fact that the identifiers are modified by the data controller to be replaced by a new random identifier does not remove their uniqueness, which makes it possible to follow an individual when browsing a site that integrates the Google Analytics feature.

In the present case, these identifiers may also be combined with other information, such as the address of the website visited, metadata relating to the browser and operating system and the time and data relating to the visit to the website. Moreover, the communication of an IP address, even if truncated, can contribute to the subsequent re-identification of the individual concerned. This combination of information enables to reinforce their discriminatory nature insofar as [REDACTED] has all this information associated with the unique identifier.

For this reason, when several elements are combined, they can make it possible to individually identify visitors to the [REDACTED] website, on which Google Analytics is implemented. It is not required to know the actual visitor's name or (physical) address since, in accordance with recital 26 of the GDPR, such singling out of individuals is sufficient to make the visitor identifiable.

Should it be decided otherwise, the scope of the right to data protection, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, would be undermined as it

would allow companies to specifically single out individuals along with personal information (such as when they visit a specific website) while denying them any right of protection against such singling out. Such a restrictive view that would undermine the level of protection of individuals is also not in line with the case law of the Court of Justice of the European Union, which repeatedly ruled that the scope of the GDPR has to be understood in a very wide manner (see, for example, C-439/19, paragraph 61).

Moreover, in [REDACTED], in the context of using Google Analytics, and under some Google account settings, Google is informed that a user connected to a Google account has visited a particular website. Personal data related to this account is then collected, including the name of its user, and linked to the unique identifier assigned as part of the Google Analytics feature. All data related to this user can therefore be attributed to an identified individual.

As a result, it must be considered that the data in question should be regarded as personal data within the meaning of Article 4 of the GDPR.

IV. On the breach of the obligation to transfer users' data to non-adequate countries in accordance with the appropriate safeguards

Article 44 of the GDPR states: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

Chapter V of the Regulation provides for various tools to ensure a level of protection substantially equivalent to that guaranteed within the European Union, pursuant to Article 44 of the Regulation:

- adequacy decisions (Article 45);
- appropriate safeguards (Article 46);

In the absence of an equivalent level of protection, it establishes derogations for specific situations (Article 49).

In the present case, it must be verified whether the export of personal data to the United States of America comply with Article 44 GDPR and, in particular, whether the export was based on one of these grounds, and if it was, if the relevant measures were taken.

4.1 Adequacy decisions

In its judgement of 16 July 2020 (C-311/18), the Court of Justice of the European Union invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the European Union-US Privacy Shield, without maintaining its effects.

In the absence of another relevant adequacy decision, the transfers in question may not be based on Article 45 of the GDPR.

4.2 Appropriate safeguards

Article 46.1 of the Regulation provides that "*In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*"

Article 46.2 of the Regulation provides that "*The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: [...] (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).*"

4.2.1 Standard data protection clauses

In the present case, the company and Google have entered into standard contractual clauses for the transfer of personal data to the United States (Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors). These clauses are in line with those published by the European Commission in Decision 2010/87/EU.

In this context, it must be emphasised that standard contractual clauses are a transfer tool within the meaning of Chapter V of the Regulation and were not challenged as such by the Court of Justice in its judgement of 16 July 2020 (C-311/18). However, the Court considered that it stemmed from the contractual nature of these clauses that they could not be binding on the authorities of third countries. In particular, 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*" (C-311/18, point 126, emphasis added).

A further analysis of the legal situation of the USA is not required though, as the CJEU has already provided such analysis in its aforementioned judgement. Indeed, the Court found that the surveillance programmes in question do not correlate to the minimum safeguards arising from the principle of proportionality under Union law, such that the surveillance programmes based on these provisions cannot be regarded as limited to what is strictly necessary (point 184). Moreover, the Court found that the legal framework in question did not confer on data subjects rights actionable in the courts against the US authorities, from which it follows that these persons have no right to an effective remedy (point 192).

The analysis of the CJEU is relevant in the present case, since Google LLC (as importer of the data to the USA) is to be qualified as a provider of electronic communications services within the meaning of 50 US. Code § 1881(b)(4) and is therefore subject to surveillance by US.

intelligence services in accordance with 50 US. Code § 1881a (“FISA 702”). Google LLC therefore has the obligation to provide the US government with personal data when requested FISA 702.

As can be seen in the Google Transparency Report, Google LLC is regular subject to such access requests by US. intelligence services.

The Court of Justice declared, on one hand, the adequacy decision with the United States of America invalid due to the access possibilities of US intelligence services, and, on the other hand, that the conclusion of SCCs cannot by themselves ensure a level of protection as required by Article 44 GDPR as the guarantees they provide are left unapplied when such access requests are taking place. Indeed, the CJEU concluded the following: *"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"* (point 133).

4.2.2 Implementation of additional safeguards

In its recommendations 01/2020 of 18 June 2021, the European Data Protection Board (EDPB) has clarified that where the assessment of the law and/or practices in force of the third country may impinge on the effectiveness of the appropriate safeguards of the transfer tools the exporter is relying on, in the context of his specific transfer, which is the case here following the assessment by the CJEU, the exporter has to either suspend the transfer or implement adequate supplementary measures. The EDPB notes in this respect that *"Any supplementary measure may only be deemed effective in the meaning of the CJEU judgement "Schrems II" if and to the extent that it – by itself or in combination with others - addresses the specific deficiencies identified in the assessment of the situation in the third country as regards its laws and practices applicable to the transfer"* (point 75).

Measures to supplement standard data protection clauses can be classified into three categories: contractual, organisational and technical (see point 47 of Recommendations 01/2020).

With regard to contractual measures, the EDPB noted that such measures: *"[...] may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country may provide [...]. 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 [...]"* (point 99, emphasis added).

As regards organisational measures, the EDPB highlighted that *"[...] Selecting 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" (point 128, emphasis added).

With regard to technical measures, the EDPB pointed out that "[...] These measures will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools and are, in particular, capable of impinging on the contractual guarantee of an essentially equivalent level of protection against access by the public authorities of that third country to that data" (point 77, emphasis added). It added that "The measures listed [in the guidelines] 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. 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" (point 79, emphasis added).

4.2.3 Supplementary measures implemented by Google

Google LLC, as the data recipient, has adopted contractual, organisational and technical measures to supplement the standard data protection clauses. [REDACTED]

Taking the considerations of the CJEU and the EDPB into account, it must now be verified whether or not the supplementary measures adopted by Google LLC are effective, meaning they address the specific issue of access possibilities of US intelligence services.

With regard to the *legal and organisational measures* adopted, it must be noted that neither the notification of users – should such notification even be permissible – nor the publication of a Transparency Report or a publicly available „policy on handling government requests” in fact prevent or reduce access possibilities of US intelligence services. Furthermore, it remains unclear how Google LLC’s „careful review of each request” on its permissibility is effective as supplementary measure, considering that according to the CJEU, permissible (legal) requests of US intelligence services are not in line with the requirements of the European Data Protection Law.

With regard to the *technical measures* adopted, it should be noted that it has not been clarified, either by Google LLC or by the company, how the measures described – such as the protection of communications between Google's services, the protection of data in transit between data centres, the protection of communications between users and websites, or “on-site security” – in fact prevent or reduce the possibilities of access by US intelligence services on the basis of the US legal framework.

As far as encryption technologies are concerned – such as for „data at rest” in data centres, as specifically mentioned by Google LLC as technical measure – it has to be noted that Google LLC as data importer nonetheless has an obligation to grant access or to turn over imported

personal data in their possession, including any cryptographic keys necessary to render the data intelligible (see Recommendations 01/2020, point 81). In other words: As long as Google LLC has the possibility to access the data of natural persons in clear text, such technical measure cannot be deemed effective in the present case.

As far as Google LLC brings forward that „(t)o the extent Google Analytics Data for measurement transferred by website owners is personal data, it would have to be regarded as pseudonymous”, it must be noted that universal unique identifiers (UUIDs) do not fall under the definition of Article 4.5 of the GDPR. While pseudonymisation may be a privacy-enhancing technique, the unique identifiers have, as already outlined above, the specific intention to single out users, not to act as safeguard. Apart from this, it has also been outlined above why the combination of unique identifiers with other elements (such as browser or device meta data) and the possibility to link such information to a Google Account in any case make an individual identifiable.

Therefore, the supplementary measures adopted, as presented by Google, are not effective insofar as none of them addresses the specific issues in the present case, meaning none of them prevent access possibilities of US intelligence services or render these accesses ineffective.

4.3. The derogations provided for in Chapter V of the Regulation

The company asserted that, the transfer of the data at issue outside the European Union is not currently based on any other tool provided for by Article 49 of the GDPR.

4.4. Conclusion

Therefore, it must be concluded that the company cannot invoke any of the tools provided for in Chapter V of the Regulation to justify the transfer of personal data of visitors to its website, and in particular unique identifiers, IP addresses, browser data and metadata, to Google LLC in the United States.

Accordingly, with this transfer of data, the company undermines the level of personal data protection of data subjects as guaranteed in Article 44 of the GDPR.

Consequently, [REDACTED], located at [REDACTED], is hereby ordered to do the following, within one (1) month of notification of this decision, that might be renewed once, and subject to any measures it may have already implemented:

- bring the data processing activity under the Google Analytics service into compliance with Articles 44 et seq. of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, notably by ceasing processing activities which relate to the current version of the tool Google Analytics;
- provide supporting documentation to the CNIL confirming that the aforementioned request has been complied with within the time limit.

At the end of that period, if [REDACTED] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if [REDACTED] has not complied with this order by the end of that period, a rapporteur will be appointed to request the restricted committee to issue one of the penalties provided for by Article 20 of the French Data Protection Act of 6 January 1978, as amended.

The Chair

[REDACTED]

**Decision [REDACTED] ordering the company on
[REDACTED] to comply**

(No. [REDACTED])

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-258C of 12 October 2020 of the Chair of the CNIL instructing the General Secretary to carry out, or have carried out, an audit of the data processing activities accessible from the domain [REDACTED] or concerning personal data collected from this domain;

Having regard to referral No. [REDACTED];

Having regard to the other exhibits;

I. The procedure

[REDACTED] (hereinafter "the company" or [REDACTED]), whose registered office is located at [REDACTED], is a retailer of perfumery and beauty products in specialized stores.

On 19 August 2020, the Commission nationale de l'informatique et des libertés (French data protection authority, hereinafter "CNIL") received a complaint (no. [REDACTED]) relating to the transfer of personal data of the complainant (represented by [REDACTED]), to the United States of America, collected during his visit to the website [REDACTED]. [REDACTED] has filed 101 complaints in the 27 Member States of the European Union and the three other members of the European Economic Area (EEA) against 101 data controllers alleged to transfer personal data to the United States.

Pursuant to decision [REDACTED] of the CNIL Chair dated [REDACTED], a CNIL delegation carried out a documentary audit by sending a questionnaire to [REDACTED] on [REDACTED] and a request for further information on [REDACTED]. The company replied in letters [REDACTED]. The questionnaires concerned the transfer of data of

visitors to the French language version of the website [REDACTED], which uses the Google Analytics service.

[REDACTED], the company informed the CNIL that it had decided to integrate the Google Analytics functionality on its website [REDACTED] and that the statistics obtained via Google Analytics concerned individuals in several member states of the European Union. The processing activity resulting from the integration of the Google Analytics functionality on its website therefore appears to meet the definition of cross-border processing within the meaning of Article 4.23.b) of the GDPR.

[REDACTED]
[REDACTED]
[REDACTED].

Pursuant to Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "GDPR" or the "Regulation"), [REDACTED], the CNIL informed all European supervisory authorities of its competence to act as lead authority regarding the cross-border processing implemented by the company, this competence deriving from the fact that the company's principal place of business is located in France.

Within the meaning of Article 4, point 22 of the GDPR, [REDACTED] data protection authorities are concerned, namely the authorities [REDACTED]
[REDACTED].

On 28 January 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

This draft decision did not give rise to any relevant and reasoned objections.

II. On the data processing in question and the responsibility for processing

The responses [REDACTED] sent to the audit delegation revealed that the company integrated the Google Analytics feature on the website [REDACTED]. This feature has been implemented for the purpose of measuring its audience and the producing of aggregated and anonymous statistical data.

[REDACTED]
[REDACTED]
[REDACTED]

Google Analytics works by including a piece of JavaScript code on the pages of a website. When a user visits a webpage, this code triggers the uploading of a JavaScript file and then performs the tracking operation for Google Analytics. The tracking operation consists of recovering data relating to the query through various means and sending this information to the Google Analytics servers.

Website managers who integrate the Google Analytics service may send instructions to Google for the processing of data collected through Google Analytics. These instructions are

transmitted through the tag manager that manages the tracking code they have integrated into their website and through the tag manager settings. The website manager can apply different settings, for example, regarding the data retention period. The Google Analytics feature also allows website managers to monitor and maintain the stability of their website, for example by keeping them informed of certain events such as a peak in audience or the fact that there is no traffic at all. Google Analytics also allows website managers to measure and optimise the effectiveness of advertising campaigns conducted using other [REDACTED] tools.

In this context, Google Analytics collects among other things the user's http query and information about the user's browser and operating system, among other things. [REDACTED]

[REDACTED] an http request, for any page, contains details of the browser and the device making the query, such as the domain name and browser information such as its type, referer, and language. Google Analytics stores and reads cookies on the user's browser to evaluate the user's session and other information on the query.

When this information is collected, it is transmitted to the Google Analytics servers. [REDACTED]
[REDACTED] all data collected through Google Analytics are hosted in the United States.

Thus, data collected on the [REDACTED] website via Google Analytics are transferred to the United States.

As regards these transfers, it appears from the exhibits that the contract between [REDACTED]
[REDACTED] concerning the Google Analytics feature refers to an appendix entitled Google Ads Data Processing Terms. This appendix contains standard contractual clauses governing the transfer of personal data to the United States of America under the Google Analytics service.

[REDACTED] it has implemented additional legal, organisational and technical measures to regulate data transfers under the Google Analytics service.

All of these elements show that, by deciding to implement the Google Analytics feature on this website for evaluation and optimisation purposes, the company managing the website [REDACTED] determined the means and purposes of the collection and processing of the data obtained further to the integration of Google Analytics on its website and should be considered the data controller within the meaning of Article 4.7 of the GDPR.

III. On the qualification of personal data

It can be established that the data collected under the Google Analytics feature and transferred to the United States of America constitute personal data.

Article 4.1 of the GDPR defines personal data as "*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.*"

It should be noted that online identifiers, such as IP addresses or information stored in cookies can commonly be used to identify a user, particularly when combined with other similar types

of information. This is illustrated by Recital 30 GDPR, according to which the assignment of online identifiers such as IP addresses and cookie identifiers to natural persons or their devices may "*leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*" In the particular case where the controller would claim to not have the ability to identify the user through the use (alone or combined with other data points) of such identifiers, he would be expected to disclose the specific means deployed to ensure the anonymity of the collected identifiers. Without such details, they cannot be considered anonymous.

Therefore, it is necessary to examine to what extent the implementation of Google Analytics on a website allows the website manager and [REDACTED] to render a data subject (a visitor of the website in question) identifiable.

The responses sent by [REDACTED] or [REDACTED] and the general functioning of Google Analytics revealed that the following categories of data are processed under the Google Analytics feature:

- data linked to a visitor's customer account ("card codes"), if the visitor is logged in to his or her account at the time of the visit, this data being pseudonymized;
- an identifier of the visitor cookie Google Analytics;
- the visitor's IP address.

The company explains that the IP addresses are truncated.

With regard to visitor identifiers, it should be noted that these are unique identifiers intended to differentiate individuals and thus identify them by allowing the company in question and Google to be able to "recognize" them later. This makes it possible, for example, to track an individual's navigation on a site that integrates the Google Analytics feature. In the present case, these identifiers may also be combined with other information, such as the address of the website visited, metadata relating to the browser and operating system and the time and data relating to the visit to the website. Moreover, the communication of an IP address, even if truncated, can contribute to the subsequent re-identification of the individual concerned. This combination of information enables to reinforce their discriminatory nature insofar as Google has all this information associated with the unique identifier.

For this reason, when several elements are combined, they can make it possible to individually identify visitors to the [REDACTED] website, on which Google Analytics is implemented. It is not required to know the actual visitor's name or (physical) address since, in accordance with recital 26 of the GDPR, such singling out of individuals is sufficient to make the visitor identifiable.

Should it be decided otherwise, the scope of the right to data protection, guaranteed by Article 8 of the Charter of Fundamental Rights of the European Union, would be undermined as it would allow companies to specifically single out individuals along with personal information (such as when they visit a specific website) while denying them any right of protection against such singling out. Such a restrictive view that would undermine the level of protection of individuals is also not in line with the case law of the Court of Justice of the European Union, which repeatedly ruled that the scope of the GDPR has to be understood in a very wide manner (see, for example, C-439/19, paragraph 61).

Moreover, [REDACTED] in the context of using Google Analytics, and under some Google account settings, Google is informed that a user connected to a Google account has visited a particular website. Personal data related to this account are then collected, including the name of its user, and linked to the unique identifier assigned by Google Analytics. All the data related to this user can therefore be attributed to an identified individual.

As a result, it must be considered that the data in question should be regarded as personal data within the meaning of Article 4 of the GDPR.

IV. On the breach of the obligation to transfer users' data to non-adequate countries in accordance with the appropriate safeguards

Article 44 of the GDPR states: "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*"

Chapter V of the Regulation provides for various tools to ensure a level of protection substantially equivalent to that guaranteed within the European Union, pursuant to Article 44 of the Regulation:

- adequacy decisions (Article 45);
- appropriate safeguards (Article 46);

In the absence of an equivalent level of protection, it establishes derogations for specific situations (Article 49).

In the present case, it must be verified whether the export of personal data to the United States of America comply with Article 44 GDPR and, in particular, whether the export was based on one of these grounds, and if it was, if the relevant measures were taken.

4.1 Adequacy decisions

In its judgement of 16 July 2020 (C-311/18), the Court of Justice of the European Union invalidated Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, in accordance with Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection afforded by the European Union-US Privacy Shield, without maintaining its effects.

In the absence of another relevant adequacy decision, the transfers in question may not be based on Article 45 of the GDPR.

4.2 Appropriate safeguards

Article 46.1 of the Regulation provides that "*In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an*

international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

Article 46.2 of the Regulation provides that "*The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: [...] (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).*"

4.2.1 Standard data protection clauses

In the present case, the company and Google have entered into standard contractual clauses for the transfer of personal data to the United States (Google Ads Data Processing Terms: Model Contract Clauses, Standard Contractual Clauses for Processors). These clauses are in line with those published by the European Commission in Decision 2010/87/EU.

In this context, it must be emphasised that standard contractual clauses are a transfer tool within the meaning of Chapter V of the Regulation and were not challenged as such by the Court of Justice in its judgement of 16 July 2020 (C-311/18). However, the Court considered that it stemmed from the contractual nature of these clauses that they could not be binding on the authorities of third countries. In particular, 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*" (C-311/18, point 126, emphasis added).

A further analysis of the legal situation of the USA is not required though, as the CJEU has already provided such analysis in its aforementioned judgement. Indeed, the Court found that the surveillance programmes in question do not correlate to the minimum safeguards arising from the principle of proportionality under Union law, such that the surveillance programmes based on these provisions cannot be regarded as limited to what is strictly necessary (point 184). Moreover, the Court found that the legal framework in question did not confer on data subjects rights actionable in the courts against the US authorities, from which it follows that these persons have no right to an effective remedy (point 192).

The analysis of the CJEU is relevant in the present case, since Google LLC (as importer of the data to the USA) is to be qualified as a provider of electronic communications services within the meaning of 50 US. Code § 1881(b)(4) and is therefore subject to surveillance by US. intelligence services in accordance with 50 US. Code § 1881a ("FISA 702"). Google LLC therefore has the obligation to provide the US government with personal data when requested FISA 702.

As can be seen in the Google Transparency Report, Google LLC is regular subject to such access requests by US. intelligence services.

The Court of Justice declared, on one hand, the adequacy decision with the United States of America invalid due to the access possibilities of US intelligence services, and, on the other hand, that the conclusion of SCCs cannot by themselves ensure a level of protection as required by Article 44 GDPR as the guarantees they provide are left unapplied when such access requests are taking place. Indeed, the CJEU concluded the following: "*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*" (point 133).

4.2.2 Implementation of additional safeguards

In its recommendations 01/2020 of 18 June 2021, the European Data Protection Board (EDPB) has clarified that where the assessment of the law and/or practices in force of the third country may impinge on the effectiveness of the appropriate safeguards of the transfer tools the exporter is relying on, in the context of his specific transfer, which is the case here following the assessment by the CJEU, the exporter has to either suspend the transfer or implement adequate supplementary measures. The EDPB notes in this respect that "*Any supplementary measure may only be deemed effective in the meaning of the CJEU judgement "Schrems II" if and to the extent that it – by itself or in combination with others - addresses the specific deficiencies identified in the assessment of the situation in the third country as regards its laws and practices applicable to the transfer*" (point 75).

Measures to supplement standard data protection clauses can be classified into three categories: contractual, organisational and technical (see point 47 of Recommendations 01/2020).

With regard to contractual measures, the EDPB noted that such measures: "*[...] may complement and reinforce the safeguards the transfer tool and relevant legislation of the third country may provide [...]. 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 [...]*" (point 99, emphasis added).

As regards organisational measures, the EDPB highlighted that "*[...] Selecting 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*" (point 128, emphasis added).

With regard to technical measures, the EDPB pointed out that "*[...] These measures will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR transfer tools and are, in particular, capable of impinging on the contractual guarantee of an essentially equivalent level of protection*

against access by the public authorities of that third country to that data" (point 77, emphasis added). It added that "The measures listed [in the guidelines] 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. 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" (point 79, emphasis added).

4.2.3 Supplementary measures implemented by Google

Google LLC, as the data recipient, has adopted contractual, organisational and technical measures to supplement the standard data protection clauses. [REDACTED]

Taking the considerations of the CJEU and the EDPB into account, it must now be verified whether or not the supplementary measures adopted by Google LLC are effective, meaning they address the specific issue of access possibilities of US intelligence services.

With regard to the *legal and organisational measures* adopted, it must be noted that neither the notification of users – should such notification even be permissible – nor the publication of a Transparency Report or a publicly available „policy on handling government requests” in fact prevent or reduce access possibilities of US intelligence services. Furthermore, it remains unclear how Google LLC’s „careful review of each request” on its permissibility is effective as supplementary measure, considering that according to the CJEU, permissible (legal) requests of US intelligence services are not in line with the requirements of the European Data Protection Law.

With regard to the *technical measures* adopted, it should be noted that it has not been clarified, either by Google LLC or by the company, how the measures described – such as the protection of communications between Google's services, the protection of data in transit between data centres, the protection of communications between users and websites, or “on-site security” – in fact prevent or reduce the possibilities of access by US intelligence services on the basis of the US legal framework.

As far as encryption technologies are concerned – such as for „data at rest” in data centres, as specifically mentioned by Google LLC as technical measure – it has to be noted that Google LLC as data importer nonetheless has an obligation to grant access or to turn over imported personal data in their possession, including any cryptographic keys necessary to render the data intelligible (see Recommendations 01/2020, point 81). In other words: As long as Google LLC has the possibility to access the data of natural persons in clear text, such technical measure cannot be deemed effective in the present case.

As far as Google LLC brings forward that „(t)o the extent Google Analytics Data for measurement transferred by website owners is personal data, it would have to be regarded as

pseudonymous”, it must be noted that universal unique identifiers (UUIDs) do not fall under the definition of Article 4.5 of the GDPR. While pseudonymisation may be a privacy-enhancing technique, the unique identifiers have, as already outlined above, the specific intention to single out users, not to act as safeguard. Apart from this, it has also been outlined above why the combination of unique identifiers with other elements (such as browser or device meta data) and the possibility to link such information to a Google Account in any case make an individual identifiable.

Therefore, the supplementary measures adopted, as presented by Google, are not effective insofar as none of them addresses the specific issues in the present case, meaning none of them prevent access possibilities of US intelligence services or render these accesses ineffective.

4.3. The derogations provided for in Chapter V of the Regulation

The company asserted that, the transfer of the data at issue outside the European Union is not currently based on any other tool provided for by Article 49 of the GDPR.

4.4. Conclusion

Therefore, it must be concluded that the company cannot invoke any of the tools provided for in Chapter V of the Regulation to justify the transfer of personal data of visitors to its website, and in particular unique identifiers, IP addresses, browser data and metadata, to Google LLC in the United States.

Accordingly, with this transfer of data, the company undermines the level of personal data protection of data subjects as guaranteed in Article 44 of the GDPR.

Consequently, [REDACTED], is hereby ordered to do the following, within one (1) month of notification of this decision, that might be renewed once, and subject to any measures it may have already implemented:

- bring the data processing activity under the Google Analytics service into compliance with Articles 44 et seq. of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, notably by ceasing processing activities which relate to the current version of the tool Google Analytics;
- provide supporting documentation to the CNIL confirming that the aforementioned request has been complied with within the time limit.

At the end of that period, if [REDACTED] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

Conversely, if [REDACTED] has not complied with this order by the end of that period, a rapporteur will be appointed to request the restricted committee to issue one of the penalties provided for by Article 20 of the French Data Protection Act of 6 January 1978, as amended.

The Chair

[REDACTED]

The President

Letter with acknowledgment of receipt



Examination of the case:

Paris, on **16 MARS 2022**

No./Ref. :

Complaint no.

(to be referenced in all correspondence)

Mr. Managing Director,

This is further to the exchanges that took place between my services and the legal manager of the [REDACTED] (hereinafter the [REDACTED] in the context of the examination of [REDACTED] complaint, which had been transmitted to us by the German data protection authority of Schleswig-Holstein pursuant to the cooperation procedures between European authorities (Articles 56.1 and seq. of the General Data Protection Regulation "GDPR").

This complaint concerned the difficulties encountered by [REDACTED] with the exercise of his right to access to his personal data concerning him and his right to erasure.

Indeed, the complainant indicates having exercised his right to access with the [REDACTED] services by email dated September 21st, 2020 addressed to [REDACTED]. He indicates having then requested the deletion of his data by an email dated December 28th, 2020 sent to [REDACTED]. His requests have finally been taken into account solely after the intervention of CNIL's services.

First, your services specify that the contact address [REDACTED] used for dealing with requests relating to the exercise of the individuals' rights, has been replaced by a secured tool for managing customer requests called [REDACTED]. They add that although this address keeps on being monitored by your customer relations department, it would now refer applicants, such as [REDACTED] to the Ariane tool for the processing of such requests.

Yet, I recall you that Article 12.2 GDPR requires the data controller to facilitate the exercise of data subjects rights.

Therefore, individuals who have already exercised their rights by electronic means should not have to reiterate their requests by another mean.

RÉPUBLIQUE FRANÇAISE

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

Second, concerning more specifically [REDACTED] access request, I note that your services haven't been able to find back the complainant's request neither on the electronic address [REDACTED] nor on the [REDACTED] tool, prior to the communication from our part of its registration number. This request has thus only been processed further to our intervention.

Concerning [REDACTED]; erasure request, your company indicates that the latter being exercised to the electronic address used for responding to his access request [REDACTED] it would have been automatically archived without your services being aware of it. Your services argue that it is possible that such request has suffered from the health situation which "*severely and rapidly overloaded [your] customer services in an unusual and prolonged way*".

Your services now confirm having erased the complainant's data from your commercial tools and your email campaigns, provided however that the data concerning his last booking from 2018 are not yet entitled to the purge in your accounting and billing tools. I note that a response in this regard has been concomitantly transmitted to [REDACTED]

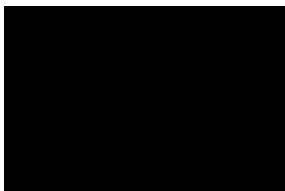
I remind you that it belongs to the data controller to follow up on requests relating to data subjects rights and to inform the latter of the measures taken in respond to these requests "*without undue delay and in any event within one month of receipt of the request*" (Article 12.3 GDPR).

Finally, I note that your company "*regularly raises [its] teams' awareness and updates [its] processes to provide the best possible response and satisfaction to [its] customers*" and in this regard, a common procedure to the requests relating to the exercise of the rights, including notably response templates validated by your data protection offer, as well as an annual awareness-raising of your teams has been put in place.

Nonetheless, all of the elements exposed above lead me, in agreement with other European data protection authorities concerned, **to issue reprimands to the [REDACTED] on its obligations provided under Articles 12.2 and 12.3 GDPR, in accordance with the provisions of Article 58.2.b) of the GDPR.**

I specify that this decision, which closes [REDACTED]'s complaint, does not preclude the CNIL from using, notably in case of new complaints, all its other powers that are granted by the GDPR and by the French law of January 6th, 1978 as amended.

Yours Sincerely,



This decision may be appealed to the French Council of State within two months of its notification.

The President

LETTER RECOMMANDÉE AVEC AR

N°AR : [REDACTED]



Examination of the case:

Paris, on 18th March 2022

Our Réf.: [REDACTED] RAL2 [REDACTED]

Case no. 21003605

(to be referenced in all correspondence)

Dear Mrs Director general,

I am following up on the exchanges that took place between the CNIL's departments and the previous Data Protection Officer (DPO) of [REDACTED] as part of the investigation of [REDACTED]'s complaint concerning the difficulties encountered in exercising his right to delete his online account with [REDACTED]'s services.

The complainant, who had an online account on the website [REDACTED] that he had not used since 2017, noted that, contrary to what is stated in the general terms of use, his account had not been deleted after 24 months of inactivity. He encountered difficulties in exercising his right to erasure.

This complaint concerns cross-border processing within the meaning of Article 4 of the General Data Protection Regulation (GDPR) and which is therefore part of the European cooperation mechanism pursuant to the provisions of Article 56 of the GDPR.

The exchanges with your DPO lead me to note the following elements.

1. Firstly, with regard to the lack of automatic deletion after a long period of inactivity of the customer's account, I note the occurrence of a malfunction in the automatic [REDACTED] account purging process at the end of 2019 and the impact of the current health crisis on the re-establishment of this purging functionality, which was due to be reactivated during June 2021.

Nevertheless, this situation led the company to keep its customers' personal data for longer than necessarily intended.

However, personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which they are processed (Article 5(1)(e) of the GDPR). I therefore consider that the company [REDACTED] has breached these provisions.

2. Secondly, with regard to the deletion request made by [REDACTED] in an e-mail dated January, 10th 2021, [REDACTED]'s services came back to him by e-mail dated February, 17th to ask him to provide a copy of his identity document.

RÉPUBLIQUE FRANÇAISE

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

However, in accordance with the provisions of Article 12(3) of the GDPR, the controller is obliged to respond to the person who has made a request pursuant to Articles 15 to 22 of the GDPR, indicating the measures taken in response to his or her request as soon as possible "*and in any event within one month of receiving the request*".

I therefore consider that the company failed to comply with Article 12.3 of the GDPR in that it did not provide the complainant with information on the outcome of his request within one month of receiving the request.

I note, however, that in its reply of June, 7th 2021, [REDACTED] s DPO informed the CNIL that the complainant's account and personal data had indeed been deleted in accordance with Article 17(1) of the GDPR, after the intervention of the CNIL on May, 3rd.

3. Thirdly, with regard to the request for identification, I note that [REDACTED] had made his request for deletion of his account from the e-mail address linked to it.

In your response to the CNIL, it was indicated that the request by your services for a copy of the applicant's identity document is a standard procedure applied for requests to exercise the most sensitive rights. You stated that following proven cases of attempted identity theft and an internal analysis, it is necessary to "*maintain this verification stage, particularly when requests are linked to the exercise of a right of access or a right to erasure, the processing of which may present risks (disclosure or destruction of data) for the data subjects in the event of identity theft*". Moreover, this verification would enable you to rule out any risk of homonymy.

I would remind you that while it is up to the controller to ensure that the applicant is indeed the data subject, by requiring him or her to prove his or her identity if necessary, no more data than necessary should be requested in application of the minimisation principle provided for in Article 5(1)(c) of the GDPR.

For this purpose, the level of checks to be carried out under Article 12(6) of the GDPR must therefore vary according to the nature and the context of the request. If an identity document can, for example, be requested in the event of suspected identity theft or account hacking, it seems disproportionate to systematically require it if the applicant makes the request from a secure personal space (customer account) or when the request is made from the e-mail address attached to his or her customer account.

The systematic collection of all the data mentioned on the identity document therefore appears, in the light of this provision, to be excessive and contravenes the principle of minimisation laid down by Article 5(1)(c).

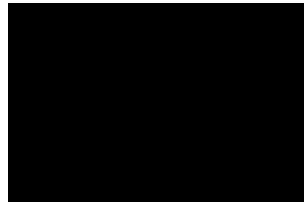
The breaches of Articles 5(1)(e), (c), and 12(3) of the GDPR lead me, in agreement with the other European data protection authorities concerned by the processing of your customers' accounts, **[REDACTED] of its obligations, in accordance with the provisions of Article 20 II of law n°78-17 of January 6th, 1978 known as "Informatique et Libertés".**

Consequently, with this letter, I remind you of the need to ensure that you respect the time limits for storing your customers' personal data and the need to respond to requests to exercise the rights within the time limit provided for by the GDPR, without systematically requiring the production of a copy of an identity document.

I nevertheless take note of the measures already taken to improve the procedures for exercising the rights of the data subjects, through the increased awareness of [REDACTED] staff and the changes to the information on your website.

I would like to point out that if this decision closes the investigation of [REDACTED]'s complaint, 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 6 January 1978 as amended.

Yours Sincerely,



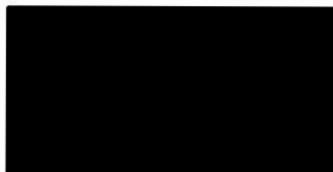
Copy to [REDACTED] [REDACTED] *Data Protection Officer*

Subject to the applicants' interest in acting, this decision may be appealed before the French State Council within a period of two months following its notification.

The Chair

Registered letter with acknowledgement of receipt

AR No: 2C 151 261 61459



Investigation of the case:

Paris, on

09 MAI 2022

Ref. No.: MLD/JTI/[REDACTED]

Referral No. [REDACTED]

(to be quoted in all correspondence)

For the attention of the Chief Executive Officer,

I am following up on the exchanges that have taken place between the departments of the *Commission Nationale de l'Informatique et des Libertés* ("CNIL" - French Data Protection Authority) and the Data Protection Officer of [REDACTED] as part of the investigation of [REDACTED]'s complaint, transmitted to the CNIL by the Bavarian Data Protection Authority.

In this case, [REDACTED] stated that he had requested, by email, on 11 December 2020, the deletion of his first name and surname, his date of birth and his email address. He specified that he wanted to receive confirmation of this deletion. On 12 December 2020, the [REDACTED] "customer support" service informed him that his request had been forwarded to the Data Protection Department and specified that said data would be immediately deleted. He was informed that he would not receive confirmation of this deletion but that he could consider this message as such.

However, the applicant continued to receive emails from [REDACTED] on the 25th of December 2020 and on the 1st and 22nd of January 2021, which is forty days after his initial request.

During discussions with your DPO, it was mentioned that at the time of the erasure request, [REDACTED] was using the services of an external partner to process exercise of rights requests and that it failed to send the request immediately despite the message sent to the applicant to confirm that the data would be deleted. Your DPO states that the winter holiday period also probably delayed the transfer of the request to its service provider.

Your DPO has stated that since then, the applicant's personal data have been anonymised and that he has been informed of the erasure of his personal data.

He has also stated that since then, [REDACTED] has taken measures to reduce the processing times of exercise of rights requests by introducing a new priority processing process and modifying the responses made to applicants when they request a deletion so that they only receive confirmation of the erasure of personal data once such personal data have been effectively erased.

The explanations provided as to the circumstances of this isolated incident and the measures already taken to avoid repeating the facts that are the subject of this complaint have led me, in agreement with the other data protection authorities concerned by this cross-border processing, to close it.

RÉPUBLIQUE FRANÇAISE

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

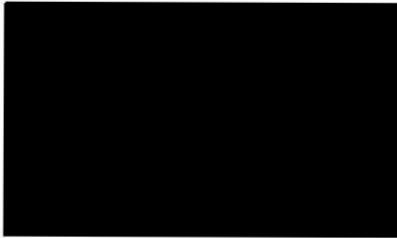
However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,



Marie-Laure DENIS

Copy to: [REDACTED] *Data Protection Officer at* [REDACTED]

The Chair**REGISTERED LETTER WITH
ACKNOWLEDGEMENT OF RECEIPT****AR No: 2C 151 961 6144 2**Investigation of the case:

Paris, on

09 MAI 2022

Ref. No. : MLD/JTI/CM [REDACTED]

Referral No. [REDACTED] and No. [REDACTED]

(to be quoted in all correspondence)

Dear Sir,

I am following up on the exchanges that have taken place between the departments of the *Commission Nationale de l'Informatique et des Libertés* ("CNIL" - French Data Protection Authority) and your company as part of the investigation of the complaints made by [REDACTED] and [REDACTED] forwarded to the CNIL by the Spanish Data Protection Authority.

In this case, [REDACTED] stated that he had requested the deletion of his [REDACTED] user account, by email on 23 February 2021, and [REDACTED] stated that he had requested the deletion of his first name and surname accessible on your website [REDACTED] by email on 29 August and on 6, 13 and 22 September 2021. Neither received a response to their request.

Based on the searches carried out by your departments as part of the investigation of these complaints, you stated that [REDACTED]'s user account has been erased since you cannot find it from his email address [REDACTED]. The applicant has confirmed to you that he is no longer able to log in to the account.

With regard to [REDACTED]'s request, it was stated that his surname and first name have been deleted from your website, that the article he published has also been deleted and that you have requested the de-indexing of the URL address referring to the deleted article from the Google search engine. You have also informed the applicant of the measures taken.

Your departments explained the absence of a response to [REDACTED]'s request by the fact that he did not have a user account, that he exercised his request for erasure through a public email address and that his e-mail must have ended up in the spam box. They added that they had taken steps to prevent such a situation from happening again.

The answers provided lead me, in agreement with the other European data protection authorities, to close these complaints.

RÉPUBLIQUE FRANÇAISE

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

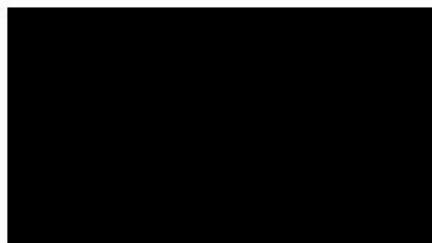
However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and by the French Data Protection Act of 6 January 1978 as amended.

Yours faithfully,



Marie-Laure DENIS

The Chair



LRAR n° LC 15196162814

Investigation of the case:

Paris,

20 MAI 2022

Ref. No.: MLD/VEI/RAL [REDACTED]

Referrals No. [REDACTED]
(to be quoted in all correspondence)

Dear Sir,

I am following up on the exchanges of letters that took place between the CNIL services and the data protection officer (DPO) of your company, as part of the investigation of several complaints relating to the processing of debtors' personal data (amicable collection files).

I. Reminder of claims and facts

With regard to referral No. [REDACTED]

The French complainant requested access to his data and received some responses. He nevertheless referred the matter to CNIL, feeling that the responses were incomplete, as the identity of the investigative agency at the origin of the data collection was not communicated to him. Following the intervention of CNIL services, his request was granted.

With regard to referral No. [REDACTED]

The data relating to the French complainant were processed by [REDACTED] based on a debt assignment agreement entered into with [REDACTED]. The complainant has repeatedly requested the source of the data concerning him, as well as its retention period and its deletion. Following discussions with CNIL services, [REDACTED] informed the complainant that his address and telephone number had been obtained from an investigative agency located in Israel. Your DPO has indicated to CNIL that the use of such an agency occurs only when the data collected from the transferring institution turns out to be inaccurate.

In addition, the complainant was informed of the "exceptional" closure of his case and that his data will be deleted after a period of six years from that closure. Your DPO justified this period by the fact that your company is "*legally required to keep this data for anti-money laundering purposes for a minimum of five years.*"

With regard to referral No. [REDACTED]

In this complaint submitted by the Polish Data Protection Authority, pursuant to Article 56.1 of the General Data Protection Regulation (GDPR), the complainant challenged the lawfulness of the processing of data concerning him by [REDACTED] and requested its erasure. He indicated that he was not a debtor and had never been a client of the ceding company. [REDACTED].

RÉPUBLIQUE FRANÇAISE

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

From the complaint and the exchanges with your company's DPO, the following details emerge:

- after unsuccessfully attempting to contact the debtor concerned, [REDACTED] appealed to an investigative agency, which sent it the contact details of the complainant on 13 July 2018;
- on 23 July 2018, the complainant requested the erasure of the data from [REDACTED], after receiving [REDACTED]'s letter informing him of the existence of a claim concerning him;
- on 27 July 2018, he contacted [REDACTED] by email [REDACTED] to obtain information, as he claims never to have taken out a loan with [REDACTED];
- on 17 September 2018, he received another letter asking him to pay his debt;
- on 29 November 2018, during a telephone conversation with the complainant, [REDACTED]'s services noticed that this was a case of mistaken identity (same surname and first name). His telephone number was then invalidated, but no further action was taken;
- the complainant's address and telephone number were anonymised following the intervention of CNIL services on 26 August 2019 (all data relating to the complainant was replaced by crosses, thus preventing any link between the true debtor's file and the complainant);
- the complainant was informed that this measure would therefore put an end to all correspondence with him.

II. Analysis of the facts in question

1. Failure to respond to requests to exercise rights

Pursuant to Article 12.3 GDPR, the Data Controller must respond to requests from individuals exercising their rights within a maximum period of one month.

In the present case, the Polish complainant attempted to obtain information on the processing of the data and requested its erasure upon receipt of the letter of assignment of claim.

An initial, insufficient measure was taken only four months after the complainant's first request. It is only the intervention of CNIL services - over a year after the complainant's first request - which led your services to respond satisfactorily.

I also note that compliance with this obligation and taking into account the complainant's requests from the outset could have enabled your company to identify the case of mistaken identity in July 2018 and thus immediately cease the processing of data concerning the complainant.

I find that [REDACTED] has therefore disregarded Article 12.3 GDPR in that it did not respond to the complainant as soon as possible.

2. Failure to process accurate and up-to-date data

Pursuant to Article 5.1.d GDPR, the personal data processed must be accurate and, if necessary, kept up to date.

In this case, the case of mistaken identity was identified on 29 November 2018 when the Polish plaintiff disputed being a customer of the company and requested the deletion of his data. However, [REDACTED] did not take adequate measures to remove any doubt as to this homonymy and immediately delete the data concerning this non-debtor complainant.

Thus, the data relating to the complainant continued to be processed by [REDACTED] and was only anonymised after the intervention of CNIL services on 26 August 2019.

I find that [REDACTED] has therefore disregarded Article 5.1 d) GDPR in that it did not take the necessary measures to process only accurate and up-to-date data relating to a debtor and that it took the intervention of CNIL services to stop this breach.

I have noted, that following discussions with your DPO, measures have been taken to ensure that such events do not recur. Claims of mistaken identity are examined within one week, so that inaccurate data is no longer processed and that the data subjects are no longer contacted.

3. Breach of obligation to limit data retention

Pursuant to Article 5.1 e) GDPR, the data must be stored for no longer than is necessary for the purposes for which the personal data are processed.

In this case, when asked about the retention period for data concerning debtors, the DPO of your company explained that it is deleted after a period of six years from the closing of the amicable collection record concerning them because your company is "*legally required to keep this data for the purpose of combating money laundering for a minimum of five years.*"

However, I believe that the retention of data for six years from the closing of a file in response to a general legal obligation "*for the purposes of combating money laundering*" which sets it at five years (Article L561-12 of the French Monetary and Financial Code) is contrary to Article 5.1 e) GDPR.

4. Breach of the obligation to inform the data subjects

Pursuant to Article 14 GDPR, where the personal data are not directly collected from the data subject, the Data Controller is required to inform that person of the source from which the data originated as such information appears "*necessary to ensure fair and transparent processing*". This information must be communicated as soon as possible (particularly during the first contact) and within one month at the latest.

In the present case, the information on the source of the data is necessary to enable the person to understand the scope of the data processing in question and, where appropriate, to fully exercise their rights. It emerges from the aforementioned complaints and investigations that the data subjects concerned by the processing related to the amicable collection of claims are not informed of the source of their personal data when they have been collected through a third party organisation.

Indeed, when the debtors' data are collected through a third party, attaching to the letter of assignment of claim sent to the debtor a copy of the privacy policy indicating the possibility of recourse to an investigative agency, does not fulfil this obligation. The information is not accurate enough and does not provide information on the exact source of the data.

As a result, the provisions of Article 14 have been disregarded by your company.

III. Corrective measure declared by CNIL (Art. 58-2 GDPR)

Due to all of these breaches thus identified, and in agreement with the other data protection authorities concerned by this processing, the following corrective measures must therefore be imposed against [REDACTED]

- **A REPRIMAND**, in accordance with the provisions of Article 58.2 b) of the General Data Protection Regulation (GDPR) and Article 20.II of the French Data Protection Act of 6 January 1978 as amended, with regard to the obligation to respond to requests for the exercise of the rights of individuals and the obligation to process accurate and updated personal data;
- **A FORMAL NOTICE** in accordance with the provisions of Article 58.2 d) of the General Data Protection Regulation (GDPR) and Article 20.II of the French Data Protection Act within one (1) month of the notification of this Decision and subject to the measures already adopted, on the one hand, to limit to five (5) years the retention period of the debtors' data from the closure of a file and, on the other hand, to correctly inform the individuals of the origin of the data concerning them used in amicable recovery procedures.

At the end of that period, if [REDACTED] demonstrates having complied with this formal notice, it will be considered that these proceedings are closed and a letter will be sent to it to that effect.

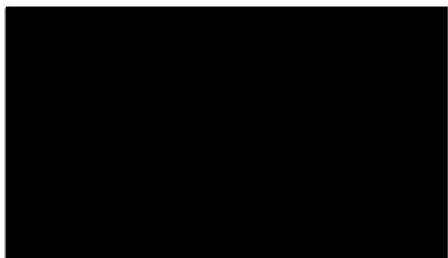
On the other hand, if [REDACTED] has not complied with this formal notice at the end of that period, I may refer to the restricted committee of the CNIL so that one or more of the sanctions provided for in Articles 20 et seq. of the French Data Protection Act of 6 January 1978, as amended, may be pronounced.

Yours sincerely,



Marie-Laure DENIS

This decision may be appealed before the French <i>Conseil d'Etat</i> within two months of its notification



Investigation of the case:

Paris, on **26 JUIL. 2022**

Ref. No.: [REDACTED]

Referral no.

(to be quoted in all correspondence)

Dear Sir,

I am following up on the complaint of [REDACTED] sent to the Commission Nationale de l'Informatique et des Libertés ("CNIL") by the Sarre data protection authority (Germany) in application of the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

[REDACTED] lodged a complaint with his local data protection authority against [REDACTED] concerning the difficulties encountered in exercising his right to erasure of his customer accounts (respectively linked to the emails [REDACTED] and [REDACTED] and to the customer identifiers [REDACTED] and [REDACTED]).

In particular, [REDACTED] stated that he had not received confirmation that his requests had been taken into account and that he had been forced to provide an identity document beforehand, even though he was connected to his customer account.

The exchanges that took place between the CNIL and the Data Protection Officer (DPO) of [REDACTED] in the context of the investigation of this complaint, revealed the following elements.

On the basis of the research carried out by your departments, it was indicated that the erasure requests relating to [REDACTED]'s two customer accounts were indeed taken into account on 18 May and 4 August 2021 and that [REDACTED] obtained confirmation of this on the same days. Supporting documentation was provided to prove this.

Concerning the prior provision of an identity document, your DPO specifies that such a document is systematically requested when the request to exercise rights is made from the form available on the [REDACTED] website without authentication on a personal account being required.

RÉPUBLIQUE FRANÇAISE

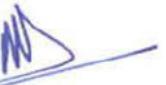
3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

In this case, it was reported that the officer in charge of the initial ticket created by [REDACTED] from his [REDACTED] customer area mistakenly redirected him to the above-mentioned form. This was due to the fact that [REDACTED] had chosen the topic "Non-compliant service", which did not correspond to the purpose of his request, instead of "GDPR" or "Account closure". Thus, it had not reached the relevant team. I note that [REDACTED]'s tools now make it easier to move a ticket from one subject line to another, and that the DPO has undertaken to raise staff awareness in this respect. I also note that an information notice under the online form now invites [REDACTED] customers to make requests to exercise their rights from their personal space in order to avoid having to provide proof of identity.

The explanations provided and the measures already taken to avoid repeating the facts that are the subject of this complaint have led me, in agreement with the other European data protection authorities, to close it.

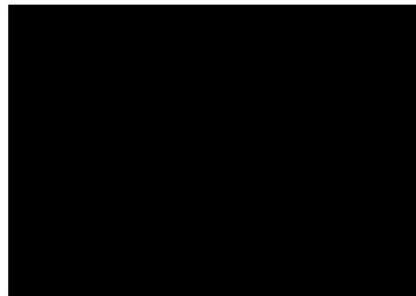
However, this decision does not preclude the CNIL from making use, particularly in the event of new complaints, of all the powers granted to it by the GDPR and by the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,



Marie-Laure Denis

Copy sent to [REDACTED], Data Protection Officer



Investigation of the case:

Paris, on **26 JUIL. 2022**

Ref: [REDACTED]

Referral no.

(to be quoted in all correspondence)

Dear Sir,

I am following up on the exchanges that took place between the Commission nationale de l'informatique et des libertés ("CNIL") and the Data Protection Officer (DPO) as part of the investigation of [REDACTED]'s complaint, which was forwarded to the CNIL by the Luxembourg data protection authority in application of 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] concerning the loss of access to his [REDACTED] cloud storage space and the difficulties encountered in exercising his rights under the GDPR.

By an email dated 15 March 2021, the latter had informed your departments of the loss of access to his storage space. Despite your answers, the problem persisted. This led him to request on 2 May 2021 a copy of the connection logs relating to his account, which he obtained on 5 May 2021, and to exercise his right to portability in order to be given the data hosted in his storage space.

I note that the loss of access to the online storage space, the reason for [REDACTED]'s requests, is no longer relevant. In this case, [REDACTED] would have changed, from the management interface of his personal space, the access identifier to his account [REDACTED] by [REDACTED] on 8 August 2020. In order to regain access to his space, it turns out that he was trying in vain to reset his password using the old login. However, problems with access to his account persisted. Alerted by CNIL as part of the investigation of this complaint, your DPO indicated on 4 February 2022 that he had contacted [REDACTED] again to ensure that he managed to reconnect to his online storage space.

As a result, [REDACTED] has since confirmed to his national data protection authority that he does not wish to pursue his access and portability requests.

RÉPUBLIQUE FRANÇAISE

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

These elements lead me, in agreement with the other European data protection authorities concerned by the processing of data of users of the [REDACTED] storage space service provided by [REDACTED] to close this complaint.

Yours sincerely



Marie-Laure Denis

Copy to [REDACTED] Data Protection Officer

Deliberation of the Restricted Committee No. SAN-2022-015 of 7 July 2022 concerning

[REDACTED]

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr. Alexandre Linden, Chair, Mr. Philippe-Pierre Cabourdin, Vice Chair, Ms. Anne Debet, Mr. Alain Dru, Mr. Bertrand du Marais, and Ms. Christine Maugüe, members;

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing Act No. 78-17 of 6 January 1978 on data protection;

Having regard to deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Authority);

Having regard to Decision No. 2020-256C of 12 May 2020 of the CNIL Chair, instructing the General Secretary to carry out, or have carried out, an investigation of the data processing activities accessible from the "[REDACTED]" domain and the [REDACTED] app, or concerning personal data collected from them;

Having regard to the decision of CNIL's Chair appointing a rapporteur before the Restricted Committee meeting of 12 April 2021;

Having regard to the report of Ms. Valérie Peugeot, Commissioner rapporteur, notified to [REDACTED] on 22 October 2021;

Having regard to the written observations made by [REDACTED] on 22 November 2021;

Having regard to the rapporteur's response to the observations notified on 15 December 2021 to the company;

Having regard to the written observations of [REDACTED] received on 17 January 2022 and the oral observations made at the Restricted Committee meeting;

Having regard to the other documents in the case file;

The following were present at the Restricted Committee session on 27 January 2022:

- Valérie Peugeot, Commissioner, her report having been heard;

In their capacity of representatives of [REDACTED]:

[...]

[REDACTED] having last spoken;

After having deliberated, the Restricted Committee adopted the following decision:

I. Facts and proceedings

1. [REDACTED] (hereinafter “[REDACTED” or “the company”) is a single-member simplified joint-stock company, whose head office is located at [REDACTED]. The company is a subsidiary of the [REDACTED]. This group generated an average revenue of [REDACTED] over 2018, 2019, and 2020. In 2019, [REDACTED] generated revenue of [REDACTED], and a net loss of approximately [REDACTED]. In 2020, [REDACTED] generated revenue of [REDACTED] and a net loss of approximately [REDACTED].
2. [REDACTED] implements a digital car-sharing vehicle rental platform which it offers to private customers and business customers. As at 9 July 2020, the company had at least [REDACTED] customers in Europe, including [REDACTED] private customers and [REDACTED] business customers in France. Its services can be accessed directly through downloading “[REDACTED]” applications (available on IOS and Android) and via the [REDACTED] website. [REDACTED] operates through its subsidiaries based notably in France, Belgium, Germany, Spain, Italy and Denmark. At the end of June 2020, [REDACTED] and its subsidiaries had [REDACTED] employees in their workforce.
3. The company has its own fleet of vehicles which the platform users can rent by creating an account on the [REDACTED] website or mobile applications. In 2019, the French subsidiary of [REDACTED] recorded [REDACTED] bookings.
4. For private customers, the company offers a round-trip shared vehicle rental offer: the customer is required to pick up and return their vehicle at the same station. The vehicles are freely accessible, in private or non-private parking areas and no [REDACTED] staff are present when a vehicle is picked up or when it is returned, the service being completely virtualized.
5. During their rental by customers, the company collects geolocation data from the vehicles, particularly in order to manage the fleet for future rentals.
6. The structure of the IT system of [REDACTED] and its subsidiaries consists of two separate platforms:
 - [REDACTED] for France, Italy and part of the activity in Belgium and Germany;
 - [REDACTED] for Spain, Denmark and the remainder of the activity in Germany.
7. Pursuant to Decision No. 2020-090C of 12 May 2020 of the CNIL Chair, an on-line investigation was conducted in order to verify compliance with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter “GDPR”) and of the French Data Protection Act No 78-17 of 6 January 1978 (hereinafter “the amended Act of 6 January 1978” or “the French Data Protection Act”) of any processing accessible from the [REDACTED] domain and the “[REDACTED]” application or involving personal data collected from them. Record No. 2020-090/1 drawn up at the end of this investigation was notified to [REDACTED] on 12 June 2020.
8. On 17 June 2020, the supervisory delegation sent a questionnaire to the company, to which the latter replied by letter dated 10 July 2020. The supervisory delegation sent additional requests

to the company, in emails dated 28 September and 26 October 2020. The company responded in emails dated 7 October and 2 November 2020.

9. In order to examine these items, the CNIL Chair appointed Valérie PEUGEOT as rapporteur on 12 April 2021, pursuant to Article 22 of the amended French Data Protection Act of 6 January 1978.
10. At the end of her investigation, the rapporteur had a bailiff notify [REDACTED], on 22 October 2021, of a report detailing the breaches of the GDPR that she considered demonstrated in this case. This report proposed to the Restricted Committee of the Commission to impose an administrative fine on the company and that the decision be made public.
11. Also attached to the report was a notice to attend the Restricted Committee meeting on 9 December 2021 informing [REDACTED] that it had one month to provide its written observations in accordance with Article 40 of Decree No. 2019-536 of 29 May 2019.
12. The company responded to the sanction report with written observations dated 22 November 2021.
13. On 30 November 2021, the rapporteur asked for time to respond to the observations made by the company. By email dated 1 December 2021, the Chair of the Restricted Committee informed the rapporteur that she had an additional eight days to submit her observations. In a letter dated the same day, the company was informed by the Chair of the Restricted Committee that it also had an eight-day time extension to file its observations.
14. By email dated 15 December 2021, the CNIL sent the company a notice to attend the Restricted Committee meeting on 27 January 2022.
15. By email of 18 December 2021, the company requested time to respond to the observations made by the rapporteur. By letter dated 21 December 2021, the Chair of the Restricted Committee informed the company that it had a time extension until 17 January 2022.
16. On 17 January 2022, [REDACTED] submitted further observations in response to those of the rapporteur.
17. The Company and the rapporteur presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

18. According to Article 56(1) GDPR, “*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*”.

19. First of all, the Restricted Committee points out that the processing operations carried out by the company in connection with its offer to business customers are not covered by this Deliberation.
20. The Restricted Committee notes that the registered office of [REDACTED] is located in France and has been registered with the Trade and Companies Register in France since the start, which leads CNIL to become the competent lead supervisory authority concerning the cross-border processing carried out by this company, in accordance with Article 56 (1) GDPR.
21. In accordance with the cooperation and coherence mechanism provided for in Chapter VII GDPR, on 15 December 2020 CNIL informed all European supervisory authorities of its competence to act as the lead supervisory authority concerning the cross-border processing carried out by the company and opening the Notification procedure for the relevant authorities in this case.
22. Pursuant to Article 60(3) GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 3rd June 2022. The Restricted Committee notes that the following supervisory authorities are concerned by this procedure: Belgium, Denmark, Spain, Italy, Baden-Wurtemberg and Berlin.
23. On the 1st of July 2022, none of the supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority. The lead supervisory authority and the supervisory authorities concerned are then deemed to be in agreement with that draft decision, pursuant to Article 60(3) GDPR.

A. On the processing in question and the quality of [REDACTED]'s data controller

24. The rapporteur points out that the data controller is defined under Article 4(7) GDPR, as "*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*".
25. The processing operations in question in these proceedings are the processing of data relating to the creation of a user account on mobile applications or the [REDACTED] website and the geolocation data collection from the rented vehicles.
26. Firstly, with regard to the responsibility for processing, it emerges from the documents in the case file that, with regard to the data collected on the mobile applications or the [REDACTED] website, the company indicates in its privacy policy that it is responsible for the processing of such personal data. Then, the company determines in particular, for all subsidiaries, the categories of data that are collected during the registration process, such as contact data. As regards the processing operations relating to geolocation data, according to the elements provided by the company, such processing operations are common to all the subsidiaries and the company has determined the different purposes (maintenance and performance of the

service, etc.). In addition, the company has established a single data retention period policy, applicable to both the company and its subsidiaries. Finally, the company has implemented two IT systems, [REDACTED] and [REDACTED], each of which is used by multiple subsidiaries, and the company can access the personal data stored in these two systems.

27. Secondly, the Restricted Committee notes that [REDACTED] does not dispute its capacity as data controller. Moreover, the possibility of joint liability of its subsidiaries is without influence on its own liability with regard to the processing in question. Indeed, this Deliberation relates to [REDACTED]'s liability for the breaches referred to and not that of its possible joint data controllers.
28. In light of these elements, the Restricted Committee finds that [REDACTED] determines the purposes and means of the processing operations relating to the creation of a user account on the mobile applications or the [REDACTED] website, and the geolocation data collection from the rented vehicles. Thus, the company must be qualified as the data controller for such processing.

B. On the breach of the obligation to ensure the personal data processed by the company are adequate, relevant and non-excessive, in accordance with Article 5(1)(C) GDPR

29. Article 5(1)(c) GDPR provides that personal data shall be “*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* (*‘data minimisation’*)”. When the data is collected on the basis of the legitimate interest, this collection must also not disproportionately cause a breach of privacy rights, with regard to the objectives pursued by the company.
30. **The rapporteur** notes that, in the context of the investigation, CNIL's supervisory delegation was informed that, during the rental of a vehicle by an individual, the company collects geolocation data every 500 metres, when the engine turns on and off, or when the doors open and close. Geolocation data is collected by systems internal to the vehicles and then transmitted by the GSM network to the service provider's IT system and then communicated to [REDACTED] platforms. The operational teams also have a button to refresh the position of the vehicle and locate it in real time.
31. The rapporteur notes that the company stated that vehicle geolocation data were collected for different purposes:
 - Ensuring maintenance and the performance of the service (making sure that the vehicle is returned to the right place, to monitor the condition of the fleet, etc.),
 - Finding the vehicle if it is stolen,
 - Assisting customers in the event of an accident.
32. The rapporteur considers that none of the purposes put forward by the company justify the almost permanent geolocation data collection during the rental of a vehicle.

33. **It is necessary to examine the relevance of the collection of this data for each of these three purposes.** First of all, the Restricted Committee points out that, when a vehicle is in the process of being rented, geolocation data from this vehicle is associated with an individual and constitutes personal data. While geolocation data are not sensitive data, within the meaning of Article 9 GDPR, they are nevertheless considered by the Article 29 Working Party (called the "WP29" which became the European Data Protection Board (EDPD) in its guidelines of 4 October 2017, to be "*highly sensitive data*". The WP29 believes that such data are considered to be sensitive data, as the term is commonly understood, insofar as they affect the enjoyment of a fundamental right. Indeed, the location data collection calls into play the freedom of movement.
34. By way of clarification, the Restricted Committee also recalls that the EDPB considered, in its guidelines 01/2020 on the processing of personal data in the context of connected vehicles and applications related to mobility (Guidelines 01/2020) that "*When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing*". These guidelines also emphasise that the location data collection is subject to compliance with the principle that location can be activated "*only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started*".
35. In this context, the Restricted Committee recalls that the assessment of compliance with the principle of data minimisation is based on the limited nature of the data processed with regard to the purpose for which it is collected. Its assessment involves an analysis of the proportionality of the personal data collection with regard to the intended purposes.
36. **Firstly, with regard to the management of the fleet of vehicles and leases, the rapporteur** considers that geolocation data collection for the entire duration of the rental is not necessary. She believes that the company may need this data to manage the start and end of the rental but that such collection is not justified over the entire rental period.
37. In defence, **the company** argues that the service offering it provides is based on immediate availability of vehicles and flexibility involving adaptation to the needs of the user that evolves during the rental period. It recalls that the system is completely virtualized and that it operates in a closed loop: the vehicle must be taken from and brought back to the same station. It argues that limiting the geolocation data collection to the scheduled end time would deprive it of the possibility of managing the fleet in a flexible manner, depending on the actual location of the vehicles. The company also contends that it is not aware in advance of the actual end time of a

rental and that customers can return the vehicle in advance simply by reporting it to the departure station. Therefore, geolocation at regular intervals would be the only way to determine the time of return of the vehicle.

38. The company argues, with regard to rental agreements, that geolocation allows it to deal with cases where the vehicle is returned outside of its departure location, in particular to be able to close the rental or recover a vehicle parked in the wrong location. In addition, it argues that it must be able to carry out supervision of the proper performance of the contract, for example during a prohibited use of the vehicle off-road or outside the national territory. Geolocation would also be necessary to supervise the entry and exit of a vehicle from urban toll areas (particularly in Madrid) and thus provide the customer with an immediate and automated billing service.
39. The company argues that it needs to know immediately whether a vehicle has been used outside the rental general terms and conditions in order to prevent the vehicle from being put back into service, for safety reasons or "*for reasons of proper administration of the service*" (including insurance).
40. **The Restricted Committee** notes the arguments put forward by the company to manage its fleet efficiently and in a flexible manner.
41. However, the Restricted Committee notes that, for this purpose, the geolocation data collection from the vehicle throughout the journey (every 500 metres when the vehicle moves but also when the motor of the vehicle is started or stopped, and when the doors are opened or closed using a badge or application) is not necessary.
42. Indeed, the Restricted Committee notes that, on the one hand, in order to return the vehicle, the engine must necessarily be shut off and, on the other hand, that this event triggers the geolocation of the vehicle. Thus, when a user starts or stops the engine of the vehicle, this vehicle sends the company the geolocation of the vehicle. If the company finds that the vehicle is back at its starting point and is closed, it can end the current rental. The geolocation of the vehicle at this time therefore makes it possible to determine whether the vehicle is at its starting point, ready to be returned. *Conversely*, the geolocation data collection during the rest of the journey is not necessary to determine whether the vehicle is returning to its departure station in order to be returned.
43. With regard to the case where the vehicle is returned elsewhere than at its departure location, it appears from the company's statements that it is not the mere geolocation of the vehicle that allows the rental to be terminated, as in the case of end of rental at the departure station. In the absence of an automatic process, the end of the rental may only take place after the customer has contacted the company. In addition, the collection of the vehicle's geolocation when the vehicle stops, at a location other than its starting point, combined with the information that it was not started again after that, makes it possible, in this case, to have data to establish the end of the rental, in connection with the telephone call from the user. In addition, the Restricted

Committee considers that, as soon as the company is aware of the customer's desire to return the vehicle to another location, it may activate geolocation in order to manage this situation.

44. With regard to compliance with the general terms and conditions of use and in particular the use of the vehicle off-road and outside the national territory, the company, questioned on this subject during the Restricted Committee session, did not provide any information relating to its effective use of geolocation data to detect such uses or to draw any consequences therefrom. In particular, it is not established whether the geolocation data is used for such purposes and, where applicable, how and in what proportions. In particular, the company has not given any indication of the actions taken when a vehicle was taken outside the national territory. The Restricted Committee underlines in this regard that, in any event, the customer may be held liable for any use of the vehicle outside of the general terms and conditions of use. The Restricted Committee notes, for the sake of completeness, that the use of regular geolocation to identify a movement of a rented vehicle off-road is not customary and raises questions of proportionality. Under these conditions, the company's desire to ensure compliance with the general conditions of use by users cannot justify geolocation of vehicles every 500 metres.
45. With regard to the use of geolocation to monitor the entry and exit of a vehicle from an urban toll area, the Restricted Committee notes first of all that this only concerns (in the States of the European Union concerned by the processing in question) the city of Madrid. Then, an almost permanent geolocation data collection on all rented vehicles, on the basis of legitimate interest, necessarily appears disproportionate to the purpose advanced, which is that of immediate, automated invoicing of costs to customers. The Restricted Committee notes that this is especially applicable with regard to the rental of vehicles in cities other than Madrid.
46. **Secondly, with regard to the fight against vehicle theft, the rapporteur** stresses that, in order to be considered proportionate, the processing of geolocation data must be made necessary for this purpose by a triggering event, such as a reported theft or suspected theft. The geolocation data of the vehicles cannot therefore be considered strictly necessary for the pursuit of the purpose related to the risk of theft, before any triggering event.
47. In its defence, **the company** argues that the geolocation data collection every 500 metres makes it possible to find the vehicle in the event of a theft or suspected theft, particularly when there are inconsistencies between the actual location of the vehicle and its scheduled return location. Indeed, geolocation would be the only effective way of meeting the legitimate objective of preventing theft. The company argues that it cannot ask customers about the location of the vehicle because, in 60% of cases identified by [REDACTED] in France in 2021, the customer is the perpetrator of the theft. In addition, the use of geolocation starting from a triggering event would at best make it possible to obtain information too late, or even no information at all. Indeed, geolocation systems would be either deactivated or rendered inoperable by placing the vehicle in an area where the signal could not be emitted (underground parking lot, etc.). Knowing the vehicle's latest known position would therefore reduce the vehicle's search area if it were stolen and no longer emitting a signal.

48. The Restricted Committee points out that, as the rapporteur found, before any triggering event, vehicle geolocation data cannot, as a rule, be regarded as strictly necessary for pursuing this purpose and their continuous collection or collection at very close intervals must be considered excessive.
49. By way of clarification, the Restricted Committee finds that the Guidelines 01/2020 state that location data can only be passed on after of a reported theft and cannot be constantly collected for the rest of the time. In this respect, the EDPB also recommends that the data controller should clearly inform the data subject that the vehicle is not permanently tracked and that geolocation data can only be collected and transmitted after the reported theft.
50. In addition, the Restricted Committee stresses that assessing if processing is limited to what is necessary, within the meaning of Article 5(1)(c) GDPR, is informed by the provisions of recital 39 GDPR, according to which, "*Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*". The existence of less intrusive means to achieve the same purposes must thus be taken into account, whether processing data by alternative means or processing less data, or processing it less frequently.
51. The Restricted Committee notes the company's observations and particularly the fact that, in 60% of theft cases in France, the theft is committed by the user of the vehicle. In such cases, this user would therefore not report, or at least not in a timely manner, the theft in question and would not provide the company with the last known position of the vehicle. However, in such cases, the company theoretically has the identity of the individual, which was verified during the user's registration process, by collecting copies of an identity document and the driving licence of that individual.
52. The Restricted Committee also notes that, in 40% of cases in France, since the user is not the thief of the vehicle, they can communicate to the company the last known position of the vehicle before it disappeared.
53. The Restricted Committee then notes that in cases where the vehicle disappears and that the last known position is not communicated by the user, the company can theoretically activate the geolocation of the vehicle remotely. It is only in cases where the vehicle is located in an area where the signal is not issued (particularly a telecommunications dead zone or underground car park), or the geolocation system has been dismantled for the theft, that the company will not have access to geolocation of the vehicle. However, the proportion of these assumptions has not been communicated by the company.
54. In this regard, the Restricted Committee considers that when the geolocation system has been knowingly rendered unusable, the information that the last known position of the vehicle represents has relative value in order to search for the vehicle.
55. Thus, the Restricted Committee points out that, in view of the above considerations, cases where, on the one hand, geolocation is the only way of knowing the last known position of the

vehicle and where, on the other hand, the last known position is actually close to the location of the vehicle, appear to be limited. In such situations, the Restricted Committee does not call into question the need to know the last known position of the vehicle thanks to the latest geolocation data. However, this assumption is not sufficient to justify the collection of all geolocation data for all users' journeys.

56. In addition, the Restricted Committee notes that other security measures could be put in place to prevent vehicle theft. Indeed, for example, no security deposit is required from the user to rent a vehicle. The Restricted Committee points out that the absence of alternative means of preventing theft, less intrusive of users' privacy, tends to reinforce the conclusion that it is disproportionate to have vehicle theft prevention be based on the near-permanent geolocation data collection.
57. In light of all of these considerations, the Restricted Committee considers that, in many use cases, the geolocation data collection every 500 metres during the car rental is not necessary for the purpose of preventing theft of the vehicle. The fact of systematically carrying out this collection for use cases where it could actually be useful, while other means of preventing and fighting theft exist, on the basis of the legitimate interest of the company, appears to cause a disproportionate breach of privacy rights. Indeed, as pointed out above, the company's collection and retention of all vehicle user journeys lead it to handling and retaining highly sensitive data.
58. Thirdly, with regard to the location of the vehicle in the event of an accident, the rapporteur argues that the geolocation data collection for this purpose can only take place from a triggering event, particularly a request for assistance by the customer, making such collection necessary.
59. In its defence, **the company** argues that limiting the triggering of geolocation to the hypothesis of a request for assistance would amount to depriving it of the possibility of providing assistance to its client even though they would be unable to request it. In addition, identifying the last known location of the vehicle would be important when the vehicle is damaged in a telecommunications "dead zone".
60. **The Restricted Committee** first points out that it is legitimate for the company to wish to assist users who are victims of a traffic accident during the rental of a vehicle. However, in order to provide such assistance to users, the company must necessarily be aware of the occurrence of an incident or accident.
61. The Restricted Committee considers that, as soon as the company becomes aware of the occurrence of an accident concerning a rented vehicle, it may geolocate this vehicle in order to, where appropriate, assist the user.
62. On the other hand, the Restricted Committee considers that geolocation every 500 meters of all vehicles throughout the rental term, prior to receiving any information relating to an accident,

is not necessary to provide assistance to a user. The near permanent geolocation data collection is therefore neither adequate nor relevant to this purpose.

63. **It follows from all of the above that the Restricted Committee considers that none of the purposes advanced by the company justify collecting geolocation data every 500 metres during the rental of a vehicle.** Such a practice is indeed very intrusive in the privacy of users insofar as it is likely to reveal their movements, their places of attendance, all of the stops made during a daily journey, which amounts to calling into question their freedom of movement. The Restricted Committee notes in this respect that it is clear from the foregoing that the company could offer an identical service without near constant geolocation data collection.
64. In addition, the Restricted Committee notes that the company has stated that its practice had evolved and that it no longer retained geolocation data histories. The Restricted Committee considers this to be a good practice, insofar as the risk of breach of privacy rights for users is less significant. However, as at the date of the investigation, the company retained a history of geolocation data in the [REDACTED] IT system.
65. The Restricted Committee therefore considers that these facts constitute a breach of Article 5(1)(c) GDPR.

C. Regarding the breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing in accordance with Article 5(1)(e) GDPR

66. According to Article 5.1(1)(e) GDPR, personal data must be “*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*”.

1. Regarding the geolocation data retention period

67. **The rapporteur** notes that it follows from the company's data retention policy that the geolocation data of individual customers is kept in an active database for the entire duration of the commercial relationship and for three years from the date of the user's last activity. During this business relationship, a customer enters into a new contract with the company for each rental of a vehicle. The rapporteur notes that the purposes for which the geolocation data is collected are related to a rental contract for a specific vehicle and not to the entire commercial relationship, which lasts until the last expression of interest in the commercial relationship by the user (in particular: a current rental or reservation, the fact of clicking on a link in a newsletter, registering for a [REDACTED] offer or a logging in to the [REDACTED] account).

68. In view of these elements, the rapporteur accuses the company of not linking the geolocation data retention period to each rental agreement but to the commercial relationship with the customer. Indeed, the date of the last activity of the user and not that of the end of the rental agreement is taken into consideration to start the data retention period. It therefore considers that the geolocation data collected during the rental of a vehicle is kept for a period exceeding the purposes for which it is processed.
69. In its defence, **the company** argues that it does not retain any history of geolocation data. It argues that each piece of geolocation data collected replaces the previously collected data, both in the [REDACTED] IT system and in the [REDACTED] IT system. Thus, only the last known position of a vehicle is maintained. Consequently, it cannot be criticised for retaining the geolocation data it collects for an excessive period of time.
70. **The Restricted Committee** recalls that the personal data retention period must be determined according to the purpose pursued by the processing. When this purpose is achieved, the data must be deleted or anonymised, or be the subject of intermediate archiving, for a specified period, when data retention is necessary for example for compliance with legal obligations or for pre-litigation or litigation purposes. The Restricted Committee also points out that the effectiveness of the implementation of a data retention period policy is the necessary counterpart to its definition and helps ensure that the data is kept in a form allowing the identification of data subjects for a period not exceeding that necessary for the purposes for which the data is processed. This also makes it possible, in particular, to reduce the risks of unauthorised use of the data in question, by an employee or by a third party (see CNIL, FR, 29 October 2021, Sanction, No. SAN-2021-019, published).
71. In this case, the Restricted Committee notes that it follows from the documents in the case file that, as at the date of the investigation by the CNIL supervisory delegation, the company retained a history of geolocation data in the [REDACTED] IT system. The geolocation data was retained, in accordance with the data retention period policy, in an active database for three years from the date of the user's last activity. The starting point for the data retention period of this data was thus linked to the end of the business relationship between the company and the user. This practice concerned part of the company's activity, i.e., data collected in countries where the [REDACTED] IT system was used (France, Italy and, partially, Belgium).
72. Yet, the Restricted Committee notes that the purposes for which geolocation data is collected are not linked to this entire business relationship but to each vehicle rental agreement. In fact, as regards, firstly, the purpose related to managing the vehicle fleet and the rental agreement, the vehicle geolocation data are no longer necessary for this purpose once the vehicle has been returned and the rental has ended. Secondly, with regard to the purpose related to the prevention of theft, geolocation data would be necessary only in the event of theft of the vehicle, the time of the investigation of the file by the competent judicial authorities or until the end of a procedure for the removal of doubt which does not result in the confirmation of the theft of the vehicle. Thirdly, with regard to the purpose of assisting users in the event of an accident, while

vehicle geolocation data may be necessary for providing an assistance service, they are no longer necessary when this service or the associated procedures end.

73. The Restricted Committee points out that, where appropriate, at the end of vehicle theft or accident procedures, geolocation data related to these procedures may be retained by the company, in particular by virtue of legal obligations or to build up evidence in the event of litigation and within the limits of the applicable limitation period. However, such data must be sorted and stored in a dedicated archive database, separate from the active database, for a period related to the intended purposes. Furthermore, the starting point for the data retention period of such data must be linked to the situations and events justifying the collection of such data and cannot, in this case, depend mechanically and systematically on the termination of the business relationship with the customer.
74. Therefore, the Restricted Committee considers that the fact that the starting point for the data retention period of geolocation data is linked not to the rental agreement but to the end of the commercial relationship with the user did not make it possible to comply with the principle that the personal data should not be kept for a period that exceeds that necessary for the purposes for which it is processed.
75. Furthermore, it follows from the evidence in the case file that the company modified its geolocation data retention policy. Thus, as at the date of the investigation by the CNIL supervisory delegation, the company retained a geolocation data history in the [REDACTED] IT system. The Restricted Committee notes that the company argues that this practice has evolved during this sanction procedure and that, now, no geolocation data history is maintained. Indeed, each piece of geolocation data collected would replace the data previously collected in the IT system. The last data collected would therefore overwrite the previous data. Therefore, at a given moment, only the last known position of the vehicle would be recorded in the IT system.
76. While the Restricted Committee takes note of this change, it notes that it was not the practice observed during the investigation.
77. The Restricted Committee concludes that the company retained the geolocation data in question for a period exceeding that necessary for the purposes for which it is processed and has thus disregarded its obligations under Article 5(1)(e) GDPR.

2. Regarding the effective implementation of the data retention policy

78. **The rapporteur** accuses the company of not complying with its data retention policy insofar as it was found during the investigation that personal data relating to users inactive for more than eight years had been present in the [REDACTED] IT system. The rapporteur maintains that certain personal data are thus retained for a period exceeding the purposes for which they are processed.

79. In its defence, **the company** argues that the data in question relates to its activity in the context of the offering of services to professionals (B2B) and that the retention policy mentioned in the report does not apply in the context of the offer to professionals.
80. **The Restricted Committee** notes that the elements of the case file do not corroborate the company's assertion.
81. In fact, firstly, the Restricted Committee notes that, in its response to CNIL dated 10 July 2020, in response to the questions of the supervisory delegation as to the number of users in the database who have not logged in to their account for more than three years, five years, eight years, the company provided extracts from the database of the [REDACTED] IT system showing personal data relating to [REDACTED] users inactive for more than eight years, [REDACTED] users inactive for more than five years, and [REDACTED] users inactive for more than three years. The Restricted Committee notes that, although the supervisory delegation requested it to "*distinguish by user type, where applicable*", the company produced a single result and did not mention the distinction between users of the services offered to individuals and professionals.
82. Secondly, the company had specified, in this same response, that "*This result [would] give rise to additional investigations to understand the reasons justifying this result.*" The Restricted Committee notes that this tends to indicate that the company had then considered this result to be non-compliant with its data retention policy.
83. Thirdly, the assertion that all the data in question relate to data collected in the context of the services offered to professionals implies that data relating to services offered to professionals and data relating to services offered to individuals are kept in the same database in the [REDACTED] IT system. Questioned on this point during the Restricted Committee meeting, the company did not explain how, in the event that all the data were kept in the same database, it would implement the necessary purges, distinguishing the data relating to services offered to professionals and the data relating to services offered to individuals.
84. The Restricted Committee considers that it is thus not demonstrated that the data in question, kept for more than three years, five years and eight years, respectively, are exclusively data collected within the context of services offered to professionals. Therefore, the data retention periods specified by the company should be applied to such data.
85. Therefore, on the basis of the elements observed by the supervisory delegation and the company's elements in response, the Restricted Committee considers that the company retained the data in question for a period exceeding that necessary for the purposes for which they are processed.
86. With regard to all of these elements, the Restricted Committee considers that the breach of Article 5(1)(e) GDPR is established.

D. Regarding the breach of the obligation to inform data subjects pursuant to Article 12 GDPR

87. Article 12(1) GDPR provides that "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing or by other means including, where appropriate, electronically. [...]*"
88. **The rapporteur** accuses the company of not providing the data subjects with the information referred to in Article 13 GDPR in a sufficiently accessible manner when conducting personal data collection for the purpose of registering with the [REDACTED] service.
89. In its defence, **the company** argues that this was a malfunction, which was corrected.
90. The Restricted Committee finds, firstly, that, with regard to the easily accessible nature of the information, the WP29 specifies, by way of illustration, in its guidelines of 11 April 2018 on transparency within the meaning of Regulation (EU) 2016/679, that "*The 'easily accessible' element 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 [...]*". "*WP29 recommends as a best practice that at the point of collection of the personal data in an online context a link to the privacy statement/ notice is provided or that this information is made available on the same page on which the personal data is collected*". These guidelines also specify that information "*should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use*". The Guidelines add that "*The data subject must not have to actively search for information covered by [Articles 13 and 14] amongst other information, such as terms and conditions of use of a website [...]*".
91. In this case, the Restricted Committee comments that, during the online investigation of 26 May 2020, by following the user registration process on the application, it was found that, in order to register, a user had to fill in various types of personal data (first name, surname, date of birth, contact details) on a registration form. It was also found that the registration form contained a link to the General Terms and Conditions of Use. In this document, there was a link to the company's privacy policy, in which the information provided for in Article 13 GDPR were presented.
92. The Restricted Committee finds that the registration form page does not allow the user to access comprehensive data protection information directly since a multi-click route was necessary to obtain it. It also notes that, in order to read information relating to the protection of personal data, individuals were required to search for it in the General Terms and Conditions of Use.

Yet, the presentation of information on the protection of personal data in a document accessible from a link in the website's General Terms and Conditions of Use cannot be regarded as satisfying the requirements of easily accessible information. Indeed, if it is not necessary to include the information referred to in Article 13 GDPR starting from the standard data collection form, it must, at the very least, present something, such as a hypertext link allowing the user to easily read all the mandatory information.

93. The Restricted Committee notes that the company brought the registration form into compliance on this point during the procedure.
94. However, it holds that, on the date of the investigation, the breach relating to the absence of information directly published or accessible on the personal data collection interface has been established with regard to the provisions of Article 12 GDPR.

III. On the sanction and publicity

95. Under the terms of Article 20(III) of the Act of 6 January 1978 amended:

"When the controller or his processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the restricted committee of the Authority with a view to the announcement, after adversarial procedure, of one or more of the following measures: [...]"

7. *With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed €10 million or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to €20 million and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83."*
96. Article 83 GDPR further states that "*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive*", before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.
97. The Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in Article 83 GDPR, such as the nature, severity, and duration of the infringement, the measures taken by the data controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority and the categories of personal data concerned by the infringement.

98. Firstly, with regard to the imposition of a fine, the Restricted Committee first considers that the company has demonstrated serious failures in terms of the protection of personal data since the breaches involve fundamental and basic principles of the GDPR, namely the principles of data minimisation, limitation of the data retention period, and accessibility of information.
99. The Restricted Committee then notes that the infringement of the rights of individuals resulting from the breach of the principle of minimisation of personal data is particularly important, given the particular nature of the geolocation data. Indeed, the company conducts near permanent geolocation data collection from users of the vehicles it rents. This near permanent geolocation data collection is particularly intrusive for rental car users. In fact, it makes it possible to track all of the journeys made by the user and identify the places where they go, thereby possibly revealing information about their behaviour and their life habits, which is likely to infringe their freedom of movement and privacy.
100. The Restricted Committee also points out that the personal data processed by the company concern about [REDACTED] users (customers and prospective customers), spread over the territory of six Member States of the European Union.
101. As regards the data retention period, on the one hand, user geolocation data are retained for an excessive period, which is not linked to the end of the rental agreement, without any particular justification. On the other hand, the company retains personal data beyond the retention periods it has defined, in disregard of the effectiveness of its retention period policy, which reveals a certain negligence in this respect.
102. In addition, it is all the more important, in the context of the geolocation data collection, since the company provides data subjects with information in a transparent and accessible manner, within the meaning of Article 12 GDPR. Indeed, data subjects must be able to understand which data is collected, how this data is used and what their rights are. The Restricted Committee notes in this respect that in view of the growth in the geolocation data collection, particularly within the framework of shared mobility services, data controllers must be particularly vigilant and transparent in the processing of this data.
103. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the breaches of Articles 5(1)(c), 5(1)(e), and 12 GDPR.
104. Secondly, with regard to the amount of the fine, the Restricted Committee recalls that Article 83(3) GDPR provides that in the event of multiple breaches, as in the case in point, the total amount of the fine may not exceed the amount set for the most serious breach. Insofar as the company is alleged to be in breach of Articles 5.1(c), 5.1(e), and 12 GDPR, the maximum fine that can be imposed is €20 million or 4% of annual worldwide turnover, whichever is higher.
105. The Restricted Committee recalls that administrative fines must be effective, proportionate and dissuasive. In particular, it considers that the organisation's activity and financial situation must

be considered when determining the sanction and, in particular, in the case of an administrative fine, its amount. In this regard, it notes that the company reports revenue in 2020 of approximately [REDACTED] with a net loss of approximately [REDACTED]

[REDACTED] The Restricted Committee also recalls that the company is a subsidiary of the [REDACTED]. This group generated an average revenue of [REDACTED] over 2018, 2019, and 2020.

106. Therefore, in view of the relevant criteria of Article 83(2) GDPR mentioned above, the Restricted Committee considers that the imposition of an administrative fine of €175,000 appears proportionate.
107. Thirdly, with regard to the publication of the sanction, the Restricted Committee considers that, in view of the plurality of the breaches identified, their severity, and the particular nature of the data concerned, the publication of this decision is justified.

FOR THESE REASONS

CNIL's Restricted Committee, after having deliberated, has decided to:

- **impose an administrative fine on [REDACTED] International in the amount of €175,000 (one hundred seventy-five thousand euros) with regard to the breaches set out in Articles 5(1)(c), 5(1)(e), and 12 of 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.**
- **Make public, on the CNIL website and on the Légifrance website, its Deliberation, which will no longer identify [REDACTED] International at the end of a period of two years following its publication.**

The Chair

Alexandre Linden

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



Registered letter with acknowledgement of receipt
AR ref. no: 2C 131 961 663 9

Investigation of the complaint:

Paris, on **02 AOUT 2022**

Our Ref.: [REDACTED]

Referral no.

(to be quoted in all correspondence)

Dear Sir/Madam,

I am following up on the complaint sent to the *Commission nationale de l'informatique et des libertés* (CNIL) by the Dutch Data protection authority [*Autoriteit Persoonsgegevens*], in application of the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

On 18 September 2021, the complainant lodged a complaint with their national Data protection authority against [REDACTED] a company established in France, concerning the security of its customers' personal data.

In particular, the complainant informed their data protection authority of the fact that [REDACTED] did not encrypt the passwords linked to its customers' personal space or at least they were accessible in clear text. They also said that passwords were sent in clear text via email when a user used the "forgot password" function on the website [REDACTED]

In the course of the exchanges that took place between the CNIL and [REDACTED] services, it was confirmed that a password management system as described by the complainant was indeed in place until 4 November 2021. I note, however, that on that date a new system was installed so that passwords are now stored in an encrypted and irreversible manner and the password recovery mechanism requires resetting the password.

The explanations provided and the measures already taken since 4 November 2021 to avoid a repeat of the events that are the subject of this complaint have led me, in agreement with the other European Data protection authorities involved, to **close this complaint**.

However, if there are any new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and the French Data Protection Act of 6 January 1978 as amended.

Yours faithfully,

On behalf of the President,

*Head of the department for the exercise of rights and
complaints*

RÉPUBLIQUE FRANÇAISE

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

The Chair



Registered letter with acknowledgement of receipt
AR No: 2c-1s-1 361 6613 7

Investigation of the case:

Paris, on

28 JUIL. 2022

Ref. No.:

Referral no.

(to be quoted in all correspondence)

Dear Sir,

I am following up on the complaint sent to the Commission nationale de l'informatique et des libertés (CNIL) by the Commission nationale pour la protection des données du Grand-Duché de Luxembourg (CNPD) in application of the provisions of Article 56.1 of the General Data Protection Regulation (GDPR).

According to the information provided by the CNPD, an email from the [REDACTED] dated 27 August 2021, entitled [REDACTED] was sent to a list of "unencrypted" email addresses.

The exchanges that have taken place between the CNIL and the Data Protection Officer (DPO) of the [REDACTED] in the context of the investigation of this complaint lead me, in agreement with the other European data protection authorities concerned, to **close this complaint**.

I have taken note of the notification of data breach No. [REDACTED] submitted to the Commission, as well as of the various steps taken by the [REDACTED] following this complaint, with regard to identifying the data breach and analysing the risk for the data subjects, or the implementation of measures to prevent the breach from being repeated (regulatory and methodological reminders to all the teams in the training department, to all the staff in the education departments of the training components and to the staff in contact with applicants, etc.).

All these elements lead me to close this complaint against the [REDACTED]

However, if there are new complaints, the CNIL reserves the right to make use of all the powers granted to it by the GDPR and the French Data Protection Act of 6 January 1978 as amended.

Yours sincerely,

Marie-Laure Denis

Copy to [REDACTED] Data Protection Officer of [REDACTED]

RÉPUBLIQUE FRANÇAISE

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

**Decision No. MED -2022-112 of 24 November 2022 serving an order on
the company [REDACTED]**

(No. MD221128)

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data, in particular Articles 56 and 60;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to referrals No. [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED], [REDACTED] and [REDACTED];

Having regard to Decision No. 2021-002C of 4 January 2021 of CNIL's Chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing of personal data implemented by the company [REDACTED] or on its behalf;

Having regard to the online investigation record no. 2021-002/1 of 7 January 2021;

Having regard to the summons for hearing report no. 2021-002/2 of 16 February 2021;

Having regard to the other exhibits;

I. The procedure

The simplified joint stock company [REDACTED], (hereinafter "the company"), located at [REDACTED] [REDACTED], publishes a website at the following URL: [REDACTED]. Dedicated to the online sale of organic cosmetic products, the company was founded in 2015 and, in this context, implements processing for the purpose of managing customers and prospects.

The company has [REDACTED] employees and generated revenue of around [REDACTED] million in 2020.

An account must be created on the site to place an order. The payment method offered by the company is payment by bank card only, which can take the form of a monthly direct debit if

the user chooses to subscribe to the “████████” offer. The user then receives a monthly box containing cosmetics products. The company’s payment provider is █████.

The company has █████ customers with an “active” status, i.e. having an ongoing subscription, and █████ customers with an “inactive” status, i.e. having terminated their subscription. In addition, it has █████ customers with an “archive” status, which corresponds to customers “inactive” for more than three years. Of the “active” clients, █████ are located in Belgium and █████ in Luxembourg.

Pursuant to Decision No. 2021-002C of 4 January 2021 of the co-chair of the French Data Protection Authority (CNIL), a CNIL delegation carried out an online investigation on 7 January 2021 regarding this company on the website █████ for the purpose of verifying the compliance of the processing implemented by the latter with all of the provisions of Act No. 78-17 of 6 January 1978 on information technology, files and freedoms as amended and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the “Regulation” or the “GDPR”).

This audit was followed by a hearing on 16 February 2021, the terms of which had been notified to the company in a letter dated 14 January 2021.

The company provided additional information by email dated 24 February and 6 April 2021.

On 14 October 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

That draft decision did not give rise to any relevant and reasoned objections.

II. The processing operations in question and responsibility for the processing

According to Article 4(7) of the GDPR, the data controller is “*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing*”.

Article 4(8) of the GDPR defines the processor as “*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*”.

By way of illustration, in guidelines 07/2020 on the concepts of data controller and processor in the GDPR, the European Data Protection Board specified that “*the nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor*” (§82).

In this case, █████ must be regarded as the data controller for the management of accounts, orders and the customer file.

The company uses a shipping service provider, [REDACTED], to deliver its packages. To this end, [REDACTED] signed on 9 October 2020 with [REDACTED] the general terms and conditions of sale concerning the organisation of the transport of packages.

To this end, [REDACTED] sends its delivery instructions and personal data concerning the package recipients. It emerges from the file that the service requested by [REDACTED] does not specifically constitute data processing but above all a delivery service; that [REDACTED] constitutes its own database from the personal data transmitted, in particular, by [REDACTED]; that it itself independently monitors the delivery and delivery of the package by contacting the recipient directly.

With regard to these elements, [REDACTED] must be considered the data controller for its delivery activity and not as a subcontractor of [REDACTED]. Therefore, the contract between the two companies is not subject to the requirements of Article 28(3) GDPR.

III. Breaches of the GDPR

Breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing

According to Article 5(1)(e) GDPR, personal data must be “*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”)*”.

At the hearing of 16 February 2021, the auditing delegation was informed that the information relating to the bank cards of subscribed users is hosted by a subcontractor, [REDACTED]. The company has a table, in its database, that contains an alias provided by [REDACTED] (“[REDACTED]”) enabling it to submit direct debit requests to [REDACTED]. This “subscriber reference” is systematically comprised of the letter “B” followed by a series of numbers. For the direct debit request to be processed, [REDACTED] needs this “subscriber reference”, as well as three other pieces of information it generates: the fields “code_cb” (bank card code), “date_val” (validation date) and “type_cb” (bank card type).

The company indicated that if a user has terminated their subscription, this “subscriber reference” is retained for a period of three months after the last direct debit. At the end of these three months, the fields “code_cb”, “date_val” and “type_cb” are deleted. With regard to the “subscriber reference”, only the letter “B” is deleted and the series of numbers is retained.

The company justifies the retention of the altered “subscriber reference” for cases where a customer wishes to re-subscribe after terminating their last subscription. They could then be asked to update their bank card data, the “subscriber reference” being necessary for updating this data. However, the company states that this is a rare case implemented in certain resubscription campaigns. Apart from these specific campaigns, the resubscription corresponds to a new order on the site, which requires entering data relating to a new bank card.

The CNIL recalls in its practical guide on retention periods (https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf) that in the absence of a text defining the retention period for the personal data concerned by the processing, “*it is the responsibility of the data controller, pursuant to the general principle of responsibility, to define said period. To do so, it must rely on the purpose for which the processing of personal data is implemented, i.e. the purpose it pursues. It is therefore necessary to identify and assess its operational needs. On the basis of these elements, a period to be applied, or, at least, the criteria for setting it (for example: the time of the business relationship) will thus be defined.*”

In this context, personal data cannot be stored for an indefinite period. Where the data is no longer necessary for the purpose for which it was collected, the data must be deleted or be subject to intermediate archiving only in the case of relevant data, when the data is necessary for compliance with legal obligations or for pre-litigation or litigation purposes. Beyond the data retention periods in intermediate archives, personal data must, unless otherwise provided, be deleted or anonymised.

The “subscriber reference” altered beyond three months cannot be used by the company to trigger a payment, as the procedure requires further information that has been deleted. However, “the subscriber reference”, even altered, can allow a single instance of correspondence between a customer’s bank data recorded in the [REDACTED] database, which keeps the bank data for a period of 13 months from the last transaction, and the customer account at the company.

The “subscriber reference” data is therefore stored without a retention period being defined and without meeting a specific purpose. These elements combined constitute a breach of Article 5-1-e of the GDPR.

Breaches of the obligation to ensure the security and confidentiality of data

Article 32 of the Regulation provides that the data controller must guarantee the security and confidentiality of the personal data it processes, in these terms: “*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: (...) b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.*”

Firstly, the delegation noted that a user’s password, generated if forgotten, is communicated clearly by email and that it is not necessary for the user to change it after the first login.

This practice generates a risk to the confidentiality of the user’s data and is contrary to the recommendations of the CNIL on this subject, which, under basic security measures, recommends that the password should never be communicated to the user in clear text by email, unless it is a temporary password or one that must be changed during the first use (<https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>).

These facts disregard, in this case, the provisions of Article 32 of the GDPR.

Secondly, the delegation was informed that the passwords of the persons having access to the back office of the after-sales department, namely the persons of the after-sales department, the statutory auditors and the chairman of the company, are created manually by the chairman of the company himself. He then hands over passwords in person in order for the data subject to register it in their password manager. If the password is forgotten, it is also the chairman of the company who must generate a new one. Lastly, on certain occasions, the password created by the chairman was communicated, by email, to the director of the after-sales department team, who was responsible for giving it to the persons concerned.

However, this measure does not make it possible to ensure that only the account holder holds the associated password, which is not liable to guarantee the traceability of access to the data (removing their attributable nature), particularly in the event of unauthorised third-party access.

According to the basic rules concerning the security of information systems, in order to be effective, a password must remain secret and individual. However, when it is known to several individuals, as in the present case, this rule is no longer respected.

To reduce the risk of disclosure of the password and respect its secrecy, it should only be known to the account holder. As such, passwords should be created or, at a minimum, renewed from the first login by the users themselves and not by a third party. It should also be possible for users to renew passwords as many times as desired. Indeed, the Commission recommends that the data controller allow the data subject to change his/her password him/herself (deliberation no. 2017-012 of 19 January 2017 adopting a recommendation on passwords).

These facts disregard, in this case, the provisions of Article 32 of the GDPR.

Lastly, the delegation was informed that during certain resubscription campaigns, the emails sent contain unique and personalised links containing the identifier of former subscribers associated with an order identifier. As such, when the person clicks on the link to resubscribe, they are automatically identified on the [REDACTED] website when the identifier and order numbers correspond to an existing customer. These links have a lifetime of one month. In addition, the emails sent to former subscribers do not contain any information on the identifier of the links.

However, links to authenticate a user pose a risk to the data contained in users' accounts. Firstly, since these links are valid for a period of one month, any person having access to the user's inbox or being able to intercept his/her emails may, within this period of one month, have access to the user account data. Secondly, the recipient of the email may decide to legitimately send this email to other persons – for example to inform them of temporary offers – without realising that the link makes it possible to log in directly to their account. Former subscribers should at least be informed of the risks of access to their personal data through resubscription campaign emails.

As such, the authentifying nature of these links, without any additional measure making it possible to ensure that it is the user account holder and without informing the recipient of the risk incurred, provides an insufficient level of security of the personal data accessible from said account.

These elements combined constitute a breach of Article 32 of the GDPR.

With regard to these three breaches, it is therefore the company's responsibility to stop sending the site login passwords, in clear text by email, without additional protection measures; to implement any measure enabling the person concerned to change his/her password to access the back office; and to stop sending by email to former subscribers links allowing automatic login to their account during commercial operations, unless additional measures are taken, in particular to ensure the authentication and information function in a robust manner.

Consequently, [REDACTED], located at [REDACTED], is hereby ordered, within three (3) months of notification of this decision, and subject to any measures it may have already adopted, to:

- **define and implement a data retention period policy that does not exceed the period necessary for the purposes for which data are collected in accordance with the provisions of Article 5(1)(e) of the GDPR**, by ensuring, when anonymising the data necessary for bank direct debits, to delete any element likely to allow re-identification by individualisation or cross-checking of any external data sets;
- **take measures to preserve the security of such data and to prevent unauthorised third parties from having access to it:**
 - by ceasing to send login passwords to the site, in clear text by email;
 - by implementing measures providing that only the holder of an account allowing access to the back office knows the password and that the passwords are created or, at least, renewed from the first login by the users themselves and not by a third party, but also by offering them the ability to renew their password at will;
 - by ceasing to send to former subscribers links allowing automatic authentication to their user account during commercial operations, except to take additional measures, in particular to ensure the authentication function and information in a robust manner.

This decision does not call for a response from you to the CNIL. However, if the breach referred to in this order is found to persist or to be repeated during subsequent investigations, I may appoint a rapporteur, within the CNIL, and refer the matter to the CNIL's restricted committee, without a new order being sent to you beforehand, so that one or more of the corrective measures provided for in Articles 20 et seq. of the Act of 6 January 1978 may be imposed, if necessary.

The Chair

Marie-Laure Denis

Deliberation of the Restricted Committee No. SAN-2023-008 of 8 June 2023 concerning

[REDACTED]

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr Alexandre Linden (Chair), Mr Philippe-Pierre Cabourdin (Vice Chair), Mr Alain Dru, Mr Bertrand du Marais and Ms Christine Maugüé (members);

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 ("GDPR");

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 et seq.;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to deliberation No. 2013-175 of 4 July 2013 concerning adoption of the CNIL's internal regulations;

Having regard to Decision No. 2020-267C of 20 October 2020 of CNIL's Chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing implemented by the company [REDACTED] or on its behalf;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 23 December 2021;

Having regard to the report of Mrs Sophie Lambremon, the commissioner rapporteur, notified to [REDACTED] on 7 July 2022;

Having regard to the written observations made by [REDACTED] on 8 August 2022;

Having regard to the other exhibits;

The following were present at the Restricted Committee session on 15 September 2022:

- Mrs Sophie Lambremon, Commissioner, heard in her report;

In the capacity of representatives of [REDACTED]:

- [...]

[REDACTED] having spoken last;

The Restricted Committee has adopted the following decision:

I. Facts and proceedings

1. [REDACTED] (hereinafter [REDACTED] or the "company") is a simplified joint-stock company incorporated in the [REDACTED], whose registered office is located at [REDACTED]. The company operates several websites to provide its customers with clairvoyance readings by chat or phone, [REDACTED]. The company employs [REDACTED] people.
2. In 2019, the company generated net revenue of [REDACTED] and net income of [REDACTED]. In 2020, its net revenue amounted to [REDACTED], with a net loss of [REDACTED].
3. A news article [REDACTED] revealed the existence of a personal data breach concerning the data stored on [REDACTED]'s server. The article claimed that the company's database had been freely accessible on the Internet until [REDACTED] 2020, since it was not protected by any specific security measures. A large amount of data, including identifying data and contact details, would therefore have been exposed.
4. On 21 January 2021, an auditing delegation from France's data protection authority "Commission nationale de l'informatique et des libertés" (hereinafter "CNIL" or the "Commission") carried out a document audit by sending a questionnaire to the company, which replied with a letter that was received on 25 March 2021.
5. An online audit was also carried out on 15 April 2021 into the [REDACTED] website published by the company. Report no. 2020-267/1 prepared at the end of the audit was served to the company on 26 April 2021. The company provided the delegation with additional information by email on 17 May and 18 June 2021.
6. An on-site audit was conducted on 15 July 2021. Report no. 2020-267/2 prepared at the end of the audit was served to the company on 21 July 2021. Subsequently, the company provided the delegation with additional information in its letters of 26 August, 20 September, 19 October and 3 November 2021.
7. [REDACTED]'s database includes the email addresses of [REDACTED] customers and [REDACTED] prospects, as can be seen from the company's observations in response.
8. In accordance with Article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority for cross-border processing implemented by [REDACTED], due to the fact that the company's single establishment is located in France. Following exchanges between the CNIL and the European data protection authorities as part of the one-stop-shop mechanism, Belgium, Luxembourg, Italy, Spain, Portugal, Bulgaria, Berlin and Ireland warranted that they were concerned by the processing operation.

9. To examine these items, the CNIL Chair appointed Ms Sophie Lambremon as rapporteur on 23 December 2021, on the basis of Article 22 of the amended Act of 6 January 1978 (hereinafter the "French Data Protection Act").
10. On 7 July 2022, the rapporteur served a report to [REDACTED] containing details of the breaches of the GDPR and French Data Protection Act that she considered had been committed in the case in point. This report contained a proposal for the Restricted Committee to impose an administrative fine on the company. It also proposed that this decision be made public and that the company no longer be identifiable by name upon expiry of a two-year period following its publication.
11. On 2 August 2022, [REDACTED] asked for time to respond to the rapporteur's report. By letter of 4 August 2022, the Chair of the Restricted Committee notified the company of its decision to deny the request.
12. The company responded to the sanction report with written observations dated 08 August 2022.
13. In a letter dated 16 August 2022, the rapporteur informed the company's counsel that the investigation was closed, pursuant to Article 40, III, amended decree no. 2019-536 of 29 May 2019.
14. In a letter dated 22 August 2022, the company was informed that the case file was on the agenda of the Restricted Committee session of 15 September 2022.
15. The rapporteur and the company presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

16. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the eight competent European supervisory authorities concerned on 4th May 2023.
17. As of 1st June 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

A. Regarding the breach of the obligation to ensure the appropriateness, relevance and non-excessive nature of the personal data processed in accordance with Article 5(1)(c) of the GDPR

18. Article 5(1)(c) of the GDPR states that personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)*".
19. **Firstly, the rapporteur** points out that the company systematically records all phone calls between telephone operators and prospects, as well as between clairvoyants and customers, with the aim of checking service quality, proving that a contract has been formed and responding to potential court orders. The rapporteur considers that this leads the company to collect data that are not limited to what is necessary in relation to the purposes pursued.
20. **In its defence, the company** indicates that it has stopped offering its customers clairvoyance readings over the phone.
21. To justify the past events, the company indicates that the recordings allowed it to check what the clairvoyants said during the readings, especially to assess their skills. In its view, recording just a sample of the readings would fail to meet its needs.
22. **The Restricted Committee** duly notes that phone-based clairvoyance readings have been stopped, which means that there are no recordings of phone calls between telephone operators and prospects, and between clairvoyants and customers.
23. However, the Restricted Committee notes that, on the day of the audit, the company systematically recorded such phone calls in full for the purpose of checking service quality, proving that a contract has been formed and responding to potential court orders.
24. The Restricted Committee notes that the company does not provide any justification for the previous need to systematically record all calls between telephone operators and prospects, as well as between clairvoyants and customers, in order to check service quality, prove that a contract has been formed and respond to potential court orders.
25. However, a controller cannot implement a personal data processing operation without first ensuring that it is necessary for fulfilling its needs, especially where it is based on a mechanism that is particularly intrusive for its employees.
26. With regard to systematically recording phone calls in full for quality control purposes, the Restricted Committee considers that the purpose of checking the quality of the service provided by the telephone operators and clairvoyants can be achieved by a less intrusive method.
27. In this respect, it notes that the implementation of an ad hoc and random system for recording only a few phone calls would allow the person responsible for quality control to have access to the information required to assess the quality of the services offered by the company.
28. Where quality control can be performed by sampling, the Restricted Committee considers that the introduction of a system for systematically recording phone calls between telephone

operators and prospects, and between clairvoyants and customers, is excessive in relation to the purpose pursued.

29. The Restricted Committee points out that it has already considered, in its deliberation no. SAN-2020-003 of 28 July 2020 with regard to a company that recorded the phone calls received by the employees in its customer service department for training purposes, that "*the company does not provide any justification for the need to record all phone calls made by the customer service department, with regard to the purpose of the processing, i.e. training for employees. (...) Although the number of recordings may vary depending on each employee and the circumstances, especially the training needs for each employee, (...) the company does not demonstrate that it has implemented, for the past and the future, a system for recording employees' phone calls that is limited to what is necessary in relation to the intended purpose. However, a controller cannot implement a personal data processing operation without first ensuring that it is necessary for fulfilling its needs, especially where it is based on a mechanism that is particularly intrusive for its employees. In light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred.*"
30. With regard to systematically recording phone calls in full for the purpose of proving that a contract has been formed, the Restricted Committee notes that, in this case, prospects disclose their telephone numbers to the company via one of its websites for the purpose of obtaining information about the proposed clairvoyance services. After enquiring about the services, telephone advisers call the prospects to provide such information and possibly arrange an appointment with a clairvoyant.
31. The Restricted Committee considers that a controller wishing to record phone calls for evidential purposes must demonstrate that it does not have any other less intrusive means to prove that a contract has been entered into remotely with the data subject.
32. In this case, the Restricted Committee considers that the existence of a contract entered into remotely can be proven by other less intrusive means.
33. Article L. 221-16 of the French Consumer Code states that when a professional contacts a consumer by telephone with a view to entering into a contract relating to the sale of a good or the provision of a service, the consumer is only bound after signing and accepting the contract on a durable physical medium.
34. Therefore, the Restricted Committee considers that once proof of an online contract following a marketing call can be provided by means of written confirmation of the proposal, it does not appear to be necessary to record phone calls between telephone operators and prospects for the purpose of obtaining proof that a contract has been executed.
35. In addition, the Restricted Committee notes that no contract is formed during phone calls between clairvoyants and customers, so the need to record those conversations is not justified for the purpose of obtaining proof that a contract has been executed.

36. With regard to systematically recording phone calls in full with a view to responding to potential court orders, the Restricted Committee notes that while it is necessary for controllers to comply with any court orders relating to the data that they are processing for their own purposes, they do not have to organise the collection of personal data in anticipation of responding to a potential court order.
37. Therefore, the Restricted Committee considers that the recording of phone calls between telephone operators and prospects, and between clairvoyants and customers, for the purpose of responding to a potential court order is not justified.
38. In light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred. The Restricted Committee duly notes that the company has stopped offering its customers clairvoyance readings over the phone, which implies that it has at least stopped recording calls between clairvoyants and customers, but this fact cannot release the company from its liability for past events.
39. **Secondly, the rapporteur** points out that customers are invited to disclose their bank account details during phone calls with telephone operators. However, the rapporteur considers that recording the part of the call relating to the collection of the customers' bank account data cannot be justified for quality control or evidential purposes.
40. **In its defence, the company** justifies that its customers' bank account data were previously collected for the purpose of booking an appointment with a clairvoyant, simplifying the payment for subsequent readings, paying for subscriptions, and combating fraud.
41. The company also indicates that implementing a mechanism to pause recordings when customers disclose their bank account data requires the development of complex systems that would entail significant financial and human resources.
42. **The Restricted Committee** notes that, on the day of the audits, the company recorded calls between telephone operators and prospects for the purpose of checking service quality, providing proof of contract formation or responding to potential court orders. During such calls, telephone operators collected the prospects' bank account data (credit card number, expiry date and security code) and informed them that collecting such data enabled them to "*participate in securing the line for only one symbolic euro*".
43. The Restricted Committee notes that the company has not implemented any specific measures to pause the recording of the phone call when collecting customers' bank account data. However, it considers that recording the part of the call relating to customers' bank account data is not useful to the company for quality control, evidential or security purposes.
44. For example, the Restricted Committee points out that it has already considered, in its deliberation no. SAN-2020-003 of 28 July 2020 with respect to a company that, when recording

phone calls for training purposes, recorded the bank account details of customers who placed orders over the phone, that "bank account details are data which, given their nature and the associated risk of fraud, must be subject to reinforced protective measures implemented by the controllers. (...) their use by unauthorised third parties in the context of fraudulent payments is likely to cause harm to the data subjects. The Restricted Committee noted that the company recorded and retained data for which it had no use in relation to the purpose of the processing concerned, namely employee training. In light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred."

45. Furthermore, the Restricted Committee considers that recording the part of the call relating to customers' bank account data is also not relevant to the purposes claimed by the company during the proceedings: booking an appointment with a clairvoyant, simplifying the payment for subsequent readings, paying for subscriptions, and combating fraud.
46. **Consequently**, and in light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred, since the company collects excessive data with regard to the purposes pursued.

B. Regarding the breach of the obligation to define and comply with a personal data retention period in proportion to the purpose of the processing in accordance with Article 5(1)(e) of the GDPR

47. According to the terms of Article 5(1)(e) of the GDPR, personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*"
48. **The rapporteur** notes that, after reading both the company's data storage period policy and privacy policy, the storage period for customer data, for the purpose of managing the business relationship and monitoring its customers, is set at three years from the end of the business relationship.
49. However, the rapporteur observes that, during the audit procedure, the company indicated that its active database contained the personal data of [REDACTED] customers who had not had a reading with a clairvoyant in more than three years, including at least [REDACTED] customers who had not had a reading with a clairvoyant in more than five years.
50. The rapporteur accuses the company of retaining its customers' data for an excessive period of time.
51. **In its defence, the company** disputes the amount stated by the rapporteur. It considers that the database contains duplicate entries. For example, it indicates that a person using a free 10-minute chat-based reading, followed by a premium chat-based reading and finally a phone-based reading is counted three times in the database.

52. Furthermore, the company accuses the rapporteur of referring to the customer's last reading with a clairvoyant when assessing the data retention period, without taking account of the fact that there is no time limit for customers to use their credit.
53. In addition, the company justifies the retention period for its customers' data of three years from the end of the business relationship by the fact that a customer may get back in contact with a clairvoyant several years after the last reading and that it is necessary for the clairvoyant to recognise a customer who has not used the company's services for a long time.
54. The company states that since the report was notified, it has implemented a purge mechanism to keep its customers' data for only one year after the end of the contractual relationship.
55. **The Restricted Committee** notes that, during the document audit, the company's active database contained the personal data of [REDACTED] customers who had not had a reading in more than three years, including [REDACTED] customers who had not had a reading in more than five years.
56. The Restricted Committee notes that, although this figure includes duplicate entries according to the company, the company has failed to notify the CNIL of the number of unique customers whose data had been kept for more than three and five years since their last reading.
57. The Restricted Committee also notes that the company justifies the data storage period by the fact that there is no time limit for customers to use their credit. However, the company did not inform the CNIL during the audit that the [REDACTED] customers who had not had a reading in more than three years, including [REDACTED] customers who had not had a reading in more than five years, are actually customers who still have credit.
58. Finally, the Restricted Committee notes that the company retained, as of the date of the audits, its customers' data for three years from the end of the business relationship and, as of the date of the Restricted Committee session, for one year from the end of the business relationship. The Restricted Committee notes that the company justifies this retention period by the need to re-identify a customer who has not used its services in a long time with the aim of providing a personalised service on the day on which that customer wishes to receive a new reading.
59. The Restricted Committee notes that the company did not inform the CNIL during the audit that these data are kept in intermediate storage.
60. The Restricted Committee considers that there is no justification to retain customers' personal data in an active database after the end of the business relationship for the aforementioned purpose. However, it considers that certain types of customer data may be retained in intermediate storage for this purpose after the end of the business relationship.
61. By way of illustration, the CNIL's reference guidelines of 23 September 2021, relating to personal data processing activities that are implemented for the purposes of managing

commercial activities, state that "*the data necessary for performing contracts are retained throughout the term of the contractual relationship. At the end of the contract, the data must be kept in intermediate storage for a reasonable period of time* if the controller needs to fulfil a legal obligation (such as to meet its accounting or tax obligations) or if the controller wishes to establish proof in the event of a dispute, and within the applicable limitation period. Therefore, the controller **must provide a dedicated archive database or logical separation in the active database after sorting the relevant data that need to be retained.** (...)"

62. **Therefore**, the Restricted Committee considers that these facts constitute a breach of the provisions of Article 5(1)(e) of the GDPR.

C. Regarding the breach of the obligation to process data lawfully in pursuance of Article 6 of the GDPR

63. According to Article 6 of the GDPR, "*processing shall be lawful only if and to the extent that at least one of the following applies:*
- (a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
- (b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
- (c) *processing is necessary for compliance with a legal obligation to which the controller is subject;*
- (d) *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
- (e) *processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*
- (f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*" »
64. **The rapporteur** notes that in the case of chat-based readings, the company retains its customers' bank account data longer than is strictly necessary for completing the transaction and facilitating subsequent payments, without obtaining their prior consent, such as on the data collection form.
65. **In its defence**, the company considers that the purpose for storing its customers' bank account data is to purchase credit and is based on the binding contract between the company and its customers. The company also considers that the storage of such data for anti-fraud purposes is based on its legitimate interest.
66. **The Restricted Committee** advises that the legal basis for processing bank account data may vary, especially depending on the purpose pursued.

67. **Firstly**, with regard to the purpose of combating fraud, the Restricted Committee considers that the legal basis for storing bank account data is, in accordance with the company's claims, the legitimate interest of the company, which is not disputed by the rapporteur.
68. In this respect, the Commission states, in its deliberation no. 2018-303 of 6 September 2018 adopting a recommendation on the processing of payment card data relating to the online sale of goods or the online provision of services, that "*the retention of payment card data beyond the completion of a transaction for the purpose of combating payment card fraud is not within the scope of the contract. It considers that such processing is in the legitimate interest of the controller, provided that it does not adversely affect the interests or rights and freedoms of individuals pursuant to Article 6(1)(f) of the GDPR, in particular by ensuring compliance with the principles of transparency and the effectiveness of the exercise of their rights by the data subjects.*"
69. **Secondly**, with regard to the purpose of topping up credit, the Restricted Committee considers that customers' bank account data are retained to provide an additional service to customers, namely that they do not have to re-enter their card number when purchasing additional credit, which goes beyond the execution of the contract.
70. Therefore, it considers that the processing of customers' bank account data for this purpose cannot be based on the contract between the customer and the company, and requires prior consent from customers.
71. By way of illustration, the Restricted Committee points out that the Commission considers, in its aforementioned deliberation, that for single payment purposes, "*the bank card number can only be collected and processed to complete a transaction as part of the performance of a contract to which the data subject is party in accordance with Article 6(1)(b) of the GDPR (contractual performance). Therefore, in the event of a contract involving a single payment, the Commission considers that the data should therefore not be retained beyond the commercial transaction time.*"
72. Still by way of illustration, the Commission indicates in the aforementioned deliberation that "*the retention of the customer's card number to facilitate any subsequent payments and potentially allow for a "one-click" purchase on the merchant's website goes beyond the performance of the contract formed. The Commission confirms that this facility constitutes an option that is independent of the initial act that led to the collection of the bank account data, and notes that such processing requires individuals to freely give their specific, informed and unambiguous consent beforehand, in pursuance of Article 6(1) of the GDPR*".
73. The Restricted Committee also advises that the Council of State, in its decision no. 429571 of 10 December 2020, held that "*the CNIL was rightly able to consider that, in general, retaining the credit card numbers of customers using e-commerce sites to facilitate their subsequent purchases should be subject to the explicit consent of those data subjects. It follows that the*

argument based on the contested decision's breach of the Regulation of 27 April 2016 must be ruled out."

74. **Consequently**, the Restricted Committee considers that there is a breach of Article 6(1) of the GDPR where the company retains its customers' bank account data beyond the completion of the transaction to facilitate the purchase of additional credit without first obtaining their consent.

D. Regarding the breach of the obligation to obtain consent prior to collecting the special categories of personal data under Article 9 of the GDPR

75. According to Article 9 of the GDPR, the processing of personal data revealing data concerning health or a natural person's sexual orientation shall be prohibited unless one of the conditions provided for in Article 9(2)(a to j) of the GDPR applies.
76. **The rapporteur** points out that clairvoyants have the possibility of adding comments to the company's customer records after a reading. The rapporteur notes that these comments include information that customers have disclosed about their health and sexual orientation. She notes that the company does not obtain the data subject's consent to use such data when creating the user account.
77. **In its defence, the company** argues that the simple fact for a person to contact a clairvoyant and spontaneously disclose sensitive information during the call constitutes a clear affirmative act of providing certain types of data and therefore constitutes consent.
78. In addition, the company maintains that most of the clairvoyants' comments do not identify the data subject, since data are pseudonymised.
79. First of all, the **Restricted Committee** notes that customers may disclose data about their health and sexual orientation to clairvoyants during readings. At the end of the reading, clairvoyants write comments in their customers' records. These records are stored in their business software. The Restricted Committee notes that clairvoyants' comments mention details about their customers' health and sexual orientation that were collected during the reading.
80. The Restricted Committee considers that the measures taken by the company do not anonymise, but simply pseudonymise customer data, insofar as the identifier associated with the comment and the information contained can be used to re-identify the customer concerned.
81. Subsequently, the Restricted Committee considers that, in the absence of any other conditions that can be invoked under Article 9(2)(b to j) of the GDPR, such processing can only be implemented where data subjects have given explicit consent to the processing of their personal data for one or more specific purposes, pursuant to Article 9(2)(a) of the GDPR. The Restricted Committee recalls that the explicit nature of consent is analysed on a case-by-case basis and depends on the context for processing sensitive data. Where the service requested by users

necessarily involves the processing of sensitive data, it is however necessary for users to be fully aware that their sensitive data will be processed and sometimes retained by the controller, which in principle implies explicit information on this point when collecting consent.

82. The Restricted Committee advises that Article 4(11) of the GDPR states that 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.
83. One the one hand, the Restricted Committee considers that the explicit nature of the consent provided for in Article 9(2)(a) of the GDPR assumes that data subjects must be able to express, by an affirmative action, their acceptance of the processing of sensitive data, demonstrating their actual consent.
84. By way of clarification, the Restricted Committee recalls that the European Data Protection Board (hereinafter the "EDPB"), in its guidelines of 10 April 2018 on consent under Regulation 2016/679, states that "*the GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for "regular" consent. As the "regular" consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the explicit consent of a data subject in line with the GDPR. The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future. However, such a signed statement is not the only way to obtain explicit consent [...]*" (Guidelines on consent under Regulation 2016/679 - WP259 rev.01 of 10 April 2018, page 21).
85. The Restricted Committee points out that it has repeatedly taken corrective measures against controllers who fail to obtain explicit consent from individuals for collecting and processing their "sensitive" data, especially in its deliberation no. 2016-405 of 15 December 2016, deliberation no. 2016-406 of 15 December 2016 and deliberation no. SAN-2017-006 of 27 April 2017 in which it considered that "*the spontaneous disclosure of such data does not release the company from its obligation to obtain express consent from the individuals who must be able to give consent to the processing of sensitive data by a clear affirmative act, thereby confirming that consent has been given with full knowledge of the facts.*"
86. Therefore, the Restricted Committee notes that the simple wish to receive a clairvoyance service and the spontaneous disclosure of sensitive information do not constitute explicit consent from the data subjects.

87. It considers that the company should have provided the individuals from whom it collects special categories of personal data with a means for giving their explicit consent by a clear affirmative act.
88. On the other hand, consent collected under the aforementioned Article 9(2)(a) of the GDPR must be read in light of the definition provided in Article 4(11) of the GDPR. In this case, it implies that for data subjects to give their valid consent, they must first be fully informed of the specific nature of the data that they are disclosing, particularly that such data may reveal their health and sexual orientation. They must also be informed of the way in which their data will be used.
89. The Restricted Committee notes that the company does not provide data subjects with specific information about the collection and processing of their health data and information relating to their sexual orientation.
90. It considers that the company should have provided data subjects with specific information, such as when creating their user account.
91. Therefore, the Restricted Committee considers that the company does not collect explicit consent from the data subjects, such that it cannot claim an exception to the restrictions on collecting and processing special categories of personal data, as provided for in Article 9(2)(a) of the GDPR.
92. **Consequently**, the Restricted Committee considers that there has been a breach of Article 9 of the GDPR insofar as the company does not obtain its customers' prior explicit consent to the collection of their health data and information about their sexual orientation.

E. Regarding the breach of the obligation for transparent information pursuant to Article 12 of the GDPR

93. Article 12(1) of the GDPR states that "*the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.*"
94. **The rapporteur** accuses the company of not providing data subjects with the information specified in Article 13 of the GDPR in a sufficiently accessible manner when collecting personal data for the purpose of creating a user account.
95. **In its defence, the company** maintains that there is no legal provision specifying the practical arrangements that the controller should take to inform its users of the processing of their

personal data. The company also states that it is separating its privacy policy from its "standard terms and conditions of sale".

96. **The Restricted Committee** advises that information is easily accessible, within the meaning of Article 12 of the GDPR, if it is provided to users without users having to actively search for that information.
97. On the one hand, the Restricted Committee notes that the form for creating a user account does not contain information on the personal data processing operations implemented by the company or any link to such information.
98. The Restricted Committee notes that, for users to access this information, they must exit the registration process and return to the homepage, scroll down to the bottom of the page, click on the company's standard terms and conditions of sale and actively search for the information relating to personal data protection.
99. When users need to perform several actions to obtain comprehensive information about data protection, the Restricted Committee holds that the information is not easily accessible.
100. On the other hand, the Restricted Committee notes that the information is contained in a document entitled "standard terms and conditions of sale", which contains both general information about the "terms and conditions of sale", the conditions for using the website, and information about the personal data processing operations implemented by the company.
101. Since the information is contained in a document that cannot be easily identified as relating to personal data protection, the Restricted Committee considers that the information is not easily accessible.
102. By way of illustration, the Restricted Committee also recalls that the EDPB, in its guidelines of 11 April 2018 on transparency, states that "*the "easily accessible" element 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 [...].*" As a best practice, the EDPB recommends that "*at the point of collection of the personal data in an online context, a link to the privacy statement / notice is provided or that this information is made available on the same page on which the personal data is collected.*" The guidelines also specify that this information "*should be clearly differentiated from other non-privacy related information such as contractual provisions or general terms of use.*" The guidelines add that "*the data subject must not have to actively search for information covered by [Articles 13 and 14] amongst other information, such as terms and conditions of use of a website [...].*"
103. **Consequently**, the Restricted Committee considers that the way in which information on personal data protection is provided on the [REDACTED] website does not meet the transparency requirements of Article 12 of the GDPR.

F. Regarding the breach of the obligation to inform data subjects pursuant to Article 13 of the GDPR

104. Article 13 of the GDPR requires the data controller to provide the data subject with various information, in particular concerning its identity and contact details, the purposes of the processing operation, its legal basis, the recipients or categories of recipients of the data, and, where applicable, the fact that the data controller intends to transfer data to a third country. In addition, the Regulation requires, where necessary to ensure "*fair and transparent processing*" of personal data in this case, that individuals are informed of the period for which the personal data will be stored, the existence of various rights that individuals have, the existence of the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.
105. **The rapporteur** observes that some information referred to in Article 13 is not provided to users on the [REDACTED] website, especially the data storage period, their right to data portability and their right to lodge a complaint with a supervisory authority.
106. Furthermore, the rapporteur notes that the sample of records submitted to the delegation shows that individuals are not informed that their call is being recorded, that they have the right to object or that the data collected during the call will be processed by the company.
107. **In its defence, the company** indicates that it is taking the necessary remedial action by including the missing mandatory information in its privacy policy. In terms of the lack of information during phone calls, the company indicates that it has stopped offering phone-based clairvoyance services.
108. **The Restricted Committee** notes that the company is currently taking action to comply with the requirement to inform data subjects and that it has stopped offering phone-based readings.
109. However, the Restricted Committee notes that the company does not dispute that, on the day of the audits, certain mandatory information under Article 13 of the GDPR was not provided to people using the [REDACTED] website and that prospects were not informed that their call was being recorded, that they had the right to object and that the data collected during the call would be processed by the company.
110. **Consequently**, the Restricted Committee considers that there has been a breach of Article 13 of the GDPR, since users will continue to be given incomplete information until such time as the company has modified the information notice on its website, and due to the lack of information provided to prospects on the day of the audits.

G. Regarding the breach of the obligation to regulate the relationship between the controller and the processor (Article 28 of the GDPR)

111. Article 28(3) of the GDPR requires that processing carried out by a processor for a controller shall be governed by a contract which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller. That contract shall also stipulate the conditions according to which the processor shall carry out the processing operations on behalf of the controller.
112. **The rapporteur** notes that two of the subcontracts and appendices provided by the company have not been signed by the service providers, while others do not include all the mandatory information.
113. **In its defence, the company** does not dispute that two subcontracts have not been signed by its service providers, and that certain mandatory information is missing from the subcontracts provided. However, the company asks the Restricted Committee to note that these subcontracts exist, which reflects its desire to comply with Article 28 of the GDPR.
114. First of all, the **Restricted Committee** notes that the appendix of the binding subcontract between the company and its processor, which attributes responsibility for any security incidents, does not include all the information provided for in Article 28(3) of the GDPR and has not been signed by the service provider.
115. Secondly, it notes that the contract between [REDACTED] and the telephone service provider does not contain a clause relating to processing by a processor, within the meaning of Article 28(3) of the GDPR.
116. Finally, it notes that the appendices to the contracts between [REDACTED] and the affiliated partners contain a subcontracting clause that does not comply with Article 28(3) of the GDPR, since it does not refer to all the mandatory information, including the obligation for the processor to process personal data only on documented instructions from the controller. It also notes that one of the appendices has not been signed by the affiliated partner.
117. The Restricted Committee considers that these facts show that contractual safeguards are unable to ensure effective protection of the personal data processed.
118. **Consequently**, the Restricted Committee considers that these facts constitute a breach of Article 28(3) of the GDPR, which the company does not dispute.

H. Regarding the breach of the obligation to ensure the security of data in pursuance of Article 32 of the GDPR

119. According to Article 32 of the GDPR: "*I. 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;*
- [...]".*

120. **Firstly, the rapporteur** points out that people can choose a single-character password when creating a user account on the [REDACTED] website. Furthermore, employees access the company's CRM system with a username and password created either by the company's CEO and the employee concerned, without any special rules concerning the complexity of the passwords or the need to automatically change the password when signing in for the first time, or by the administrator using a generator that returns a password between 9 and 12 characters, including alphanumeric and special characters.
121. **In its defence, the company** does not provide any response to the lack of rules for creating robust passwords.
122. **The Restricted Committee** recalls that, pursuant to Article 32 of the GDPR, in order to protect personal data, the controller must take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".
123. The Restricted Committee considers that the use of overly lenient rules governing password complexity, which would allow users to choose passwords that are insufficiently strong, can lead to attacks by unauthorised third parties, such as "brute force" or dictionary" attacks, which involve successively and systematically testing numerous passwords and which therefore compromise the associated accounts and the personal data contained in those accounts.
124. In this respect, the Restricted Committee notes that the need for a strong password is recommended by both the ANSSI (French National Agency for Information Systems Security) and the CNIL in its deliberation no. 2017-012 of 19 January 2017, where such a requirement is confirmed in its deliberation no. 2022-100 of 21 July 2022.
125. The Restricted Committee points out that it has repeatedly imposed financial penalties where a breach of Article 32 of the GDPR is caused by insufficient measures to guarantee the security of the data processed. Deliberations no. SAN-2019-006 of 13 June 2019, no. SAN-2019-007 of 18 July 2019 and no. SAN-2022-018 of 8 September 2022 specifically refer to weak passwords.
126. In this case, the Restricted Committee notes that the passwords for users of the [REDACTED] website may comprise a single character.
127. The Restricted Committee considers that data subjects are incurring a real risk: a third party with access to the password could access the personal data present in the data subject's account, view the credit usage history and/or change the account password without the user's knowledge.

128. Furthermore, the Restricted Committee notes the lack of strong passwords allowing company employees to access the CRM system, given that there are no complexity rules when they are created by the CEO and the employee concerned, and that there are no additional security measures when they are created by the administrator (passwords comprising 9 to 12 alphanumeric and special characters).
129. The Restricted Committee also considers that the procedure for creating passwords does not ensure data confidentiality, since when the password is created by the administrator, he/she sends it to the company's CEO, who forwards it to the relevant employee concerned, and when the password is not created by the administrator, the CEO creates it in liaison with the relevant employee.
130. These facts constitute a real risk to data subjects: an unauthorised third party with access to the password could access a large amount of personal data, including sensitive data.
131. Consequently, taking into account these risks for the protection of personal data and the privacy of individuals, the Restricted Committee considers that the measures implemented to guarantee data security in this case are insufficient.
132. As such, in light of the risks incurred by data subjects as stated above, as well as the sensitivity of certain types of data (health data, data relating to sexual orientation and bank account data), the Restricted Committee considers that the company has breached the obligations under Article 32 of the GDPR.
133. **Secondly**, the rapporteur notices that the mechanism used by the company to encrypt the bank details presents vulnerabilities (determination in advance of the vector initialisation, reuse of it and obsolescence of the library used), which does not, in view of the sensitivity of this data, ensure a level of security appropriate to the risk.
134. **In defense, the company** explains that its data processor, the company [REDACTED], should have advised it concerning the encryption of data.
135. **The restricted committee** mentions again that protection of bank details requires the implementation of increased security measures, such as encryption, in view of their highly personal nature.
136. In this case, the restricted committee notes that the documents in the file show that [REDACTED] was not in charge of encrypting the banking data of [REDACTED]'s customers, but rather of managing the information system and hosting the data.
137. The restricted committee also notices that the documents in the file show that [REDACTED] has encrypted its customers' bank details itself, and in an unsecured manner.

138. Indeed, the restricted committee observes that the MITRE (American non-profit organisation involved in particular in systems engineering and information technology) CWE (Common Weakness Enumeration) list, which lists software weaknesses, identifies generating a predictable initialisation vector with CBC mode as a vulnerability, as in this case, such as reusing an initialisation vector. The restricted committee notes that when the initialisation vector is not random but determined, the clear message is still encrypted in the same way. It is therefore possible to compare several encrypted messages and identify the clear messages to which they correspond. Moreover, by reusing the initialisation vector, this vector is common to all data encrypted with the unique key.
139. The restricted committee also notes that Mycrypt, the encryption library used by the company, was considered obsolete and removed in 2017, so that the use of this functionality is not recommended in the PHP documentation.
140. As a consequence, the restricted committee considers that the above-mentioned facts constitute an infringement of Article 32 of the GDPR, since the mechanism implemented by the company [REDACTED] to encrypt its customers' bank details does not ensure a level of security appropriate to the risk.
141. **Thirdly, the rapporteur** points out that the [REDACTED] website was accessed at the time of the audit using the "HTTP" protocol, including the page for collecting bank account data. However, "HTTP" is not a secure protocol, meaning that the site is vulnerable to attacks and allows transmissions containing personal data (including bank account data) between the user's browser and the server hosting the website to be read in plain text format.
142. **In its defence, the company** advises that it changed its "HTTP" protocol to the TLS protocol on the [REDACTED] website after receiving the report.
143. **The Restricted Committee** recalls that, pursuant to Article 32 of the GDPR, the controller must take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".
144. The Restricted Committee notes that the "HTTP" protocol is a communication protocol that does not allow for authentication of the website or encryption of the data when sent to the servers hosting the company's website, which does not guarantee the authenticity of the website viewed or the integrity and confidentiality of the data exchanged, thereby exposing the personal data processed through these pages to the risks of eavesdropping, interception or modification without the user's knowledge, which could lead to a breach of the data subjects' privacy.
145. By way of clarification, the Restricted Committee notes that the need to ensure confidentiality over the channels used to transmit personal data has been highlighted by ANSSI since 2013, especially in its "*Recommendations for the implementation of a website: achieving proficiency in the standards of browser security*", which specify that "*the implementation of HTTPS on a website or a web application is a security guarantee based on TLS to ensure the confidentiality*

and integrity of the information exchanged, as well as the authenticity of the server contacted. The absence of this guarantee can lead to many abuses without malicious intent."

146. The Restricted Committee also finds that since the publication of its "Personal Data Security" guide in 2018, the Commission has consistently recommended that the "TLS" protocol be implemented as a basic precaution, using only the most recent versions and verifying its proper implementation.
147. The Restricted Committee also holds that the personal data in question are highly personal, since they are bank account data. Therefore, taking into account the risks to the protection of the data subjects' personal data and privacy, the Restricted Committee considers that the measures deployed to guarantee data security in this case are inadequate, given that personal data are transmitted between the user's browser and the server hosting the website.
148. **Consequently**, the Restricted Committee considers that, with regard to the personal data that are subject to the processing (especially bank account data), the failure to implement the basic security measure, such as the use of the "HTTPS" protocol or another equivalent security measure, constitutes a breach of Article 32 of the GDPR. Nevertheless, the Restricted Committee notes that the company changed the protocol during the audit. However, the Restricted Committee reiterates that the remedial measures taken do not release the company from its liability for the breach observed.

I. Regarding the breach of the obligation to notify personal data breaches to the CNIL in pursuance of Article 33 of the GDPR

149. Article 4(12) of the GDPR defines a personal data breach as a "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"
150. Article 33 of the GDPR states that "*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 (...) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*" »
151. Recital 87 of the GDPR states that "*It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject*".

152. **The rapporteur** notes that the company became aware of the personal data breach on 29 September 2020 after receiving a sample of the affected data from a journalist, or no later than 30 September 2020, following its internal investigation.
153. According to the rapporteur, the personal data breach was likely to result in a risk to data subjects' rights and freedoms, particularly in light of the duration of the breach (two months and four days) and the potential number of data subjects (█████ customers and prospects in the database).
154. Consequently, the rapporteur considers that the company should have notified the existence of the personal data breach to the CNIL in phases, where applicable.
155. **In its defence, the company** acknowledges that it became aware of the existence of the security incident on 29 September 2020. However, the company indicates that access to the server in question had been closed since 10 July 2020, which brought an end to the security incident.
156. It attributes liability for the security incident to its facilities management subcontractor. The company advises that after it had asked its subcontractor to provide its developer with access to its server, its subcontractor acted outside its instructions by making the server accessible to unauthorised third parties.
157. Finally, the company disputes the number of customers and prospects in its database as claimed by the rapporteur. The company considers that the database contains the email addresses of █████ customers and █████ prospects.
158. **The Restricted Committee** recalls that, in accordance with Article 33 of the GDPR, the principle in the event of a personal data breach is to notify the supervisory authority. Controllers are only exempt from this obligation where the breach is unlikely to result in a risk to the rights and freedoms of natural persons.
159. The Restricted Committee also recalls that in the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the controller is required to notify the breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.
160. By way of illustration, the Restricted Committee indicates that the EDPB, in its guidelines on personal data breach notification of 6 February 2018, considers that "***a controller should be regarded as having become aware*** [of the personal data breach] ***when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.*** ***The GDPR requires the controller to implement all appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject (...).*** ***The controller is therefore required to take the necessary measures to***

ensure that it becomes "aware" of any breaches in a timely manner so that it can take appropriate action."

161. By way of example, "*a third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach, then there can be no doubt that it has become "aware".*"
162. Still by way of illustration, the EDPB states that "*after first being informed of a potential breach by an individual, a media organisation (...), the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation, the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.*" »
163. In this case, the Restricted Committee notes that access to the server in question was closed by the company's subcontractor as requested on 10 July 2020, because it was not suited to its needs.
164. The Restricted Committee points out that a journalist notified the company by email on 29 September 2020 of the existence of a security incident due to a port that had wrongly been opened on the server. It also notes that the journalist's email provided the company with a sample of the database that had apparently been disclosed, i.e. identification and contact data.
165. The Restricted Committee notes that the company conducted a short internal investigation on 30 September 2020, following which it concluded that the security incident could be attributed to its facilities management subcontractor, which accidentally opened a port on the server.
166. It notes that the company listed the security incident in its data breach record and identified one of the likely consequences of the breach to be the "*resale of data leading to direct marketing without the consent of the data subjects concerned by the breach*".
167. The Restricted Committee notes, however, that the company did not notify the CNIL. The company justifies this lack of notification by the fact that it would not have been able to observe the data breach, since the journalist's alert occurred after the server had been closed and that its facilities management subcontractor did not keep the connection logs for the server concerned.
168. According to the Restricted Committee, the company did not implement all the appropriate measures to immediately establish the existence of the personal data breach.
169. The Restricted Committee considers that although the company was informed of the security incident after the server had been closed, it was able to identify the existence of a data breach by comparing the sample data provided by the journalist with its own database.

170. In addition, the Restricted Committee draws attention to the delay in sending a request to the subcontractor to provide the connection logs, since that request was only made on 25 November 2020, i.e. two months after the journalist's alert.
171. In light of the foregoing, the Restricted Committee considers that, no later than 30 September 2020, which is the date of the internal investigation, the company had a reasonable degree of certainty that there was a data breach causing a risk to data subjects' rights and freedoms, especially given the duration of the breach (two months and four days) and the potential number of data subjects, i.e. [REDACTED] customers and prospects.
172. The Restricted Committee notes that the company, in its capacity as the controller, had an obligation to notify the data breach, even if the breach was caused by an error that could be attributed to the subcontractor.
173. Consequently, the Restricted Committee considers that the company breached its obligations by failing to notify the data breach to the CNIL.
174. In light of the foregoing, the Restricted Committee considers that a breach of Article 33 of the GDPR has been committed.

J. Regarding the breach of Article 82 of the French Data Protection Act

[Breach not subject to cooperation on which the supervisory authorities concerned did not have to take a position.]

175. Article 82 of the French Data Protection Act states that "*any subscribers or users of an electronic communications service must be informed in a clear and complete manner, unless they have been previously informed by the controller or its representative:*
1° Of the purpose of any action aimed at electronically accessing information already stored in their electronic communications terminal equipment, or writing information to this equipment;
2° Of how they can object to it [...]."
Such access or writing may only take place on the condition that the subscribers or users have given their consent, after receiving this information, which may result from appropriate settings in their connection device or any other device under their control (...) However, these provisions do not apply if access to the information stored in the user's end device or the storage of information in the user's end device: 1° Is for the exclusive purpose of allowing or facilitating electronic communication; 2° Or is strictly necessary for the provision of an online communication service at the express request of the user".
176. These provisions incorporate Article 5(3) 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 (called the "ePrivacy Directive") into French law.

177. **Firstly, the rapporteur** notes that the delegation reported during the online audit on 15 April 2021 that there was no banner or interface to provide information to users and obtain their consent to cookies when accessing the [REDACTED] website, even though certain cookies were placed on users' devices.
178. The rapporteur notes that, during the on-site audit on 15 July 2021, the delegation identified a cookie banner when accessing the website.
179. However, the rapporteur considers that the information displayed is unsatisfactory and does not provide data subjects with any further details about their consent, since no information is given on how to refuse trackers, the consequences of refusing trackers and their right to withdraw consent.
180. **In its defence, the company** argues that it has produced a compliant cookie banner on its website since the report was received.
181. **The Restricted Committee** recalls that, as a result of the combined provisions of Article 82 of the French Data Protection Act and Article 4 of the GDPR, tracking cookies requiring consent may, subject to the exceptions provided for by those provisions, only be used to read and write information if users freely give their consent in a specific, unambiguous and informed manner by a clear affirmative action.
182. The Restricted Committee considers that the validity of consent is consequently associated with the quality of the information received.
183. By way of clarification, the Restricted Committee indicates that the CNIL, in its guidelines on the application of Article 82 of the French Data Protection Act relating to read and write operations on a user's device, addresses the informed nature of consent by specifying that "*as a minimum, the following information must be given to users prior to obtaining their consent in order to ensure that consent is informed:*
- *The identity of the controller(s) responsible for the read or write operations*
 - *The purpose of the data read or write operations*
 - *The procedure for accepting or refusing tracking cookies*
 - *The consequences of refusing or accepting tracking cookies*
 - *The existence of their right to withdraw consent"*
184. In its recommendation of 17 September 2020 that proposes practical methods for ensuring compliance where cookies and other trackers are used, the Commission states that "*in practice, to reconcile the requirements for clear and concise information with the need to identify all the controllers, the specific and regularly updated information about those entities (identities or link to their personal data processing policy) may, for example, be provided at a second level of information. Therefore, the information can be made available from the first level, such as via a hypertext link or a button accessible from that level.*" Information relating to the identity

of the controller(s) for read and write operations may therefore be provided at a second level of information.

185. By way of illustration, the Restricted Committee also notes that the Commission, in the Questions and Answers on the CNIL's Amending Guidelines and Recommendations on "*Cookies and Other Trackers*" of 4 November 2022, states that "*for users to provide an informed indication of their consent, all the information specified in Article 2 of the guidelines on "cookies and other trackers" must be available at the time of their choice. For the first level of information, the recommendation is to clearly indicate the purposes of the cookies, allow users to access the list of controllers, such as by means of a hypertext link or a button accessible from the first level of information, inform them of their right to withdraw consent at any time and, where applicable, inform them of the consequences of refusing cookies.*"
186. The Restricted Committee notes that, on the day of the online audit, the [REDACTED] website did not have a banner to inform users about the cookies placed on their devices when accessing the website. Therefore, users were not informed of the operations carried out or were unable to give their prior consent, such as required by Article 82 of the French Data Protection Act, as clarified by Article 4 of the GDPR.
187. The Restricted Committee notes that it was only during the on-site audit on 15 July 2021 that the delegation observed the following cookie banner when accessing this website: "*We use cookies and other tracking technologies to enhance your browsing experience on our website, show you personalized content and targeted advertising, analyse our website traffic and understand where our visitors have come from*", including the "*I accept*" and "*Change my preferences*" buttons.
188. The Restricted Committee also notes that after clicking on the "*Change my preferences*" button, users are shown the following information: "*You can change your preferences and refuse certain types of cookies on your computer when navigating on our website. You can also delete cookies that are already stored on your computer, but remember that deleting such cookies may prevent you from using parts of our website.*"
189. The Restricted Committee notes that, during the on-site audit on 15 July 2021, the first level of information provided to users did not explain the possibility and procedure for refusing cookies, as well as the consequences of refusing cookies and their right to withdraw their consent.
190. The Restricted Committee notes that, when accessing the [REDACTED] website as of the date of the Restricted Committee session, the cookie banner included the following notice and the "*I accept*", "*I refuse*" and "*Change my preferences*" buttons: "*We use cookies and other tracking technologies to enhance your browsing experience on our website, show you personalized content and targeted advertising, analyse our website traffic and understand where our visitors have come from.*"

191. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 82 of the French Data Protection Act, since at the time of the online audit and until the cookie banner had been modified, users accessing the [REDACTED] website were not informed of the operations allowing access to or storage of information on their devices, in accordance with Article 82 of the French Data Protection Act and Article 4 of the GDPR, and they were therefore unable to give an informed indication of their consent.
192. **Secondly, the rapporteur** notes that during the online audit of 15 April 2021, the delegation found that three cookies requiring prior consent from users were stored on their devices as soon as they accessed the [REDACTED] website without their prior consent and before they could take any action.
193. **In its defence, the company** argues that no non-essential cookies have been stored on users' devices since the report was notified.
194. **The Restricted Committee** recalls that Article 82 of the French Data Protection Act requires consent for reading and writing information on a user's device, but provides for specific cases where certain trackers are exempt from consent: either when the tracker is for the exclusive purpose of allowing or facilitating communication by electronic means, or when the tracker is strictly necessary for providing an online communication service at the user's express request.
195. With respect to traffic measurement trackers that are exempt from consent and by way of illustration, the Restricted Committee notes that the Commission specifies in its guidelines of 17 September 2020 that "*in many cases, these measures are essential for the proper operation of the website or application, and therefore for the provision of the service. Consequently, the Commission considers that trackers whose purpose is limited to measuring traffic on the website or application, in response to different needs (performance metrics, detection of navigation issues, improvements to technical performance or usability, estimation of the required server power, analysis of the content viewed, etc.), are strictly necessary for the operation and day-to-day administration of a website (...) To remain within the limits of what is strictly necessary for providing the service, the Commission stresses that these trackers must have a purpose that is strictly limited to measuring traffic on the website or application for the publisher's sole use.*"
196. Regarding multi-purpose trackers, the Restricted Committee notes, still by way of illustration, that the Commission specifies in its guidelines of 17 September 2020 that "***the use of the same tracker for several purposes, some of which fall outside these exemptions, requires prior consent from the data subjects, according to the conditions specified in these guidelines. For example, in case of a service offered over a platform that requires user authentication (login), the service publisher may use a cookie to authenticate users without requesting their consent (because this cookie is strictly necessary to provide the online communication service). However, it may only use the same cookie for advertising purposes if data subjects have actually given their prior consent to this specific purpose.***

197. To determine whether the storage of a multi-purpose cookie on the user's device requires prior consent, the Restricted Committee considers that it is necessary to determine whether at least one of the purposes requires prior consent.
 198. In this case, the Restricted Committee notes that the company stored and read the following cookies on users' devices as soon as they accessed the [REDACTED] website without obtaining their prior consent and before they could take any action: "test_cookie", ".ga" and ".gid".
 199. The Restricted Committee notes that "test_cookie" is for advertising purposes. Therefore, it does not qualify as an exception under Article 82 of the French Data Protection Act and may not be stored on the user's device without prior consent.
 200. The Restricted Committee notes that the ".ga" and ".gid" cookies pursue several purposes, i.e. a purpose for monitoring and analysing the [REDACTED] website, and a Google-specific purpose for maintaining and protecting the Analytics service. As such, these cookies are not exclusively for the purpose of allowing or facilitating electronic communication and are not strictly necessary for providing the service. Consequently, they do not qualify as an exception under Article 82 of the French Data Protection Act and may not be stored on the user's device without prior consent.
201. Therefore, the Restricted Committee considers that storing and reading these cookies on the user's device requires prior consent from that user, according to the conditions stipulated in Article 82 of the French Data Protection Act, as clarified by Article 4(11) of the GDPR.
 202. The Restricted Committee points out that it has repeatedly imposed financial penalties for breaches of Article 82 of the French Data Protection Act where cookies requiring consent have been stored on users' devices without obtaining their consent and before users could take any action (particularly deliberations SAN-2022-023 of 19 December 2022, SAN-2022-025, SAN-2022-026 and SAN-2022-027 of 29 December 2022).
 203. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 82 of the French Data Protection Act for the acts that were identified on the day of the audits, since cookies that were subject to prior consent were stored on users' devices without their consent and before they could take any action.
 204. The Restricted Committee notes that, during the audit, [REDACTED] indicated that it had taken measures to comply with the requirements of Article 82 of the French Data Protection Act, insofar as it no longer stores a cookie that is not essential for the operation of the [REDACTED] website.

205. **Thirdly**, the rapporteur notes that, during the on-site audit on 15 July 2021, the auditing delegation found that the cookie banner on the [REDACTED] website did not allow users to refuse cookies as simply as accepting them.
206. **In its defence, the company** argues that its cookie banner will soon include a "*refuse*" button.
207. **The Restricted Committee** considers that in this case, to guarantee freedom of consent, it should be just as easy to refuse cookies as to accept them.
208. By way of clarification, the Restricted Committee indicates that the Commission, in its guidelines on the application of Article 82 of the French Data Protection Act relating to read and write operations on a user's device, specifies that "*the expression of the user's refusal must therefore not require any procedure from the user or must involve an action offering the same degree of simplicity as the action provided to express the user's consent.*"
209. The Restricted Committee notes that, as evidenced by the findings of the on-site audit on 15 July 2021, when users visited the [REDACTED] website, they could agree to the storage of cookies requiring consent with a single action by clicking on the "*I accept*" button in the cookie banner.
210. However, when it comes to refusing these cookies, the Restricted Committee notes that users had to perform no less than five actions: click on the "*Change my preferences*" button to access the cookie management interface (first click), click on the "*Functionality cookies*" tab (second click) and the "*Monitoring and performance cookies*" tab (third click), click on the "*Targeting and advertising cookies*" tab (fourth click) to decide whether to store these cookies, and click on the "*Save my preferences*" button (fifth click).
211. Therefore, the Restricted Committee considers that the process for refusing cookies failed to offer the same degree of simplicity as the process for accepting cookies, and that making the cookie refusal mechanism more complex than the acceptance mechanism is actually tantamount to discouraging users from refusing cookies and encouraging them to prefer the ease of the "*Accept all*" button. Internet users are generally prompted to visit many sites. Speed and fluidity are distinctive features of browsing on the Internet. Having to click on "*Change my preferences*" and understand how the page to refuse cookies is built is likely to discourage users, who would nevertheless like to refuse the storage of cookies. In the present case, It is not disputed that the company offered a choice between accepting and refusing cookies before adding the "*Refuse all*" button, but the methods for expressing refusal in the context of Internet browsing skews the choice in favour of consent, which affects the freedom of choice.
212. The Restricted Committee points out that it has repeatedly imposed financial penalties for breaches of Article 82 of the French Data Protection Act in cases where it was not as simple for users to refuse cookies as it was to accept them. In deliberation no. SAN-2022-023 of 19 December 2022 and deliberation no. SAN-2022-027 of 29 December 2022, the Restricted Committee considered that "*making the cookie refusal mechanism more complex than the*

acceptance mechanism is actually tantamount to discouraging users from refusing cookies and encouraging them to prefer the ease of the "Accept" button. Internet users are generally prompted to visit many sites. Speed and fluidity are distinctive features of browsing on the Internet. Having to click on "More options" and understand how the page to refuse cookies is built is likely to discourage users, who would nevertheless like to refuse the storage of cookies. In the present case, It is not disputed that the company offered a choice between accepting and refusing cookies before adding the "Refuse all" button, but the methods for expressing refusal in the context of Internet browsing skews the choice in favour of consent, which affects the freedom of choice" (also in deliberations SAN-2021-023 and SAN-2021-024 of 31 December 2021).

213. The Restricted Committee notes that, when accessing the [REDACTED] website as of the date of the Restricted Committee session, the cookie banner included the "*I refuse*" button.
214. **Consequently**, the Restricted Committee considers that there has been a breach of the provisions of Article 82 of the French Data Protection Act, as interpreted in light of the GDPR, since at the time of the online audit and until such time as the company had implemented the "*Refuse all*" button, users did not have the possibility of refusing read and/or write operations with the same degree of simplicity as accepting such operations.

III. On the sanction and publicity

215. According to Article 20(III) of the French Data Protection Act:

"When the controller or its processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this Act, CNIL's Chair may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL's Restricted Committee with a view to the imposition, after proceedings in which both sides are represented, of one or more of the following measures: [...]

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83."

216. Article 83 of the GDPR states that "*each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate*

and dissuasive", before specifying the information to be taken into account when deciding whether to impose an administrative fine and when deciding on the value of such a fine.

217. **Firstly**, on the principle of imposing a fine, the company insists in its defence that its subcontractor is liable for the security breaches and the origin of the security incident. The company states that any data that were potentially accessible do not concern highly personal data or sensitive data. Furthermore, it disputes the number of data subjects, but without specifying the exact number.
218. It also advises that no complaints had been received and considers that certain breaches cause little harm to data subjects, especially breaches of Articles 12 and 28 of the GDPR. It also emphasises the efforts that it has undertaken to align and comply with the corresponding requirements after receiving the report.
219. **First of all**, the Restricted Committee notes that, when deciding to impose an administrative fine, it must give due regard to the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the infringement, the action taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority, and the categories of personal data affected by the infringement.
220. **Furthermore**, the Restricted Committee points out the particularly high number of breaches, i.e. nine breaches under the GDPR (Articles 5(1)(c), 5(1)(e), 6, 9, 12, 13, 28, 32 and 33) and one breach under the French Data Protection Act (Article 82). Therefore, the company has demonstrated multiple failures, since the established breaches concern a large part of the personal data protection rules, including the controller's fundamental obligations (data minimisation, limitation of the data storage period, accessibility of information, and lawfulness of processing).
221. For example, systematically recording all phone calls in full between telephone operators and prospects, as well as between clairvoyants and customers, for quality control and evidential purposes is a particularly intrusive practice for data subjects.
222. Furthermore, the company failed to comply with several provisions in Article 82 of the French Data Protection Act, including a lack of information, a lack of consent for storing cookies that are not exempt from consent, and a lack of similarity between the means offered to users for accepting or refusing the option of storing cookies on their device. These facts constitute a substantial infringement of data subjects' right to privacy and the protection of their personal data.
223. By way of illustration, the Restricted Committee also points out that the company did not notify the CNIL of the data breach, even though it had all the elements to verify the existence of a breach and that it identified unauthorised direct marketing to be a probable consequence of the breach.

224. The Restricted Committee subsequently notes that some breaches concern special categories of data that are subject to strict legal regulations (health data and information about sexual orientation) and highly personal data (bank account data), for which greater care must be taken in light of the risks of fraud.
225. The Restricted Committee also advises that the company, in its capacity as the controller, is required to comply with its obligations under the GDPR. In particular, the company is required to carry out a satisfactory and regular inspection of the technical and organisational measures implemented by its processor to ensure compliance with the GDPR and particularly ensure the security of the personal data processed.
226. In this respect, the Restricted Committee notes that several basic security measures were lacking in this case, which led to a risk for data subjects. The Restricted Committee points out that the various documents governing the contractual relationship between the company and its subcontractors do not contain all the measures required by Article 28 of the GDPR, and some documents have not been signed by the service providers. These facts show that contractual safeguards are unable to ensure effective protection of the personal data processed.
227. Lastly, the Restricted Committee notes that the remedial measures implemented by the company after receiving the report, especially concerning cookies, do not release the company from its liability for the previous breaches observed.
228. Consequently, the Restricted Committee considers that there are grounds to impose an administrative fine for the breaches of Articles 5(1)(c), 5(1)(e), 6, 9, 12, 13, 28, 32 and 33 of the GDPR and Article 82 of the French Data Protection Act.
229. **Secondly**, in terms of the amount of the fine and in its defence, the company insists on the fact that it generated a net loss.
230. The Restricted Committee considers that the company's financial situation must be taken into account when determining the penalty and, in the event of an administrative fine, its amount. In this respect, it notes that [REDACTED]'s net revenue in 2020 amounted to [REDACTED], while its net loss was [REDACTED]. For information purposes, the company specified during the Restricted Committee session that its projected revenue from January to August 2022 is approximately [REDACTED].
231. Therefore, in light of the aforementioned relevant criteria of Article 83(2) of the GDPR, the Restricted Committee considers that the imposition of an administrative fine of €150,000 is justified. This fine can be broken down as follows. €120,000 for the breaches of the GDPR and €30,000 for breach of the French Data Protection Act.
232. **Thirdly**, with regard to the publication of the penalty, the company argues that such a measure would be detrimental from a business point of view.

233. The Restricted Committee considers that the publication of this decision is justified in view of the multiple breaches identified, their severity, the specific nature of the data processed and the number of data subjects.

FOR THESE REASONS

CNIL's Restricted Committee, after having deliberated, decided to:

- Impose an administrative fine on [REDACTED] in the amount of €120,000 (one hundred and twenty thousand) for the breaches of Articles 5(1)(c) and (e), 6, 9, 12, 13, 28, 32 and 33 of 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, and €30,000 (thirty thousand) for the breach of Article 82 of the French Data Protection Act.
- Publish its decision on the CNIL and Légifrance websites, which will no longer identify [REDACTED] by name at the end of a period of two years from its publication.

The Chair

Alexandre Linden

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

Summary Final Decision Art 60

Investigation

EDPBI:FR:OSS:D:2023: 802

Administrative fine Violation identified

Background information

Date of final decision:	08 June 2023
Date of broadcast:	19 June 2023
LSA:	FR
CSAs:	BE, LU, IT, ES, PT, BG, DE, IE
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 6 (Lawfulness of processing), Article 9 (Processing of special categories of personal data), Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 28 (Processor), Article 32 (Security of processing), Article 33 (Notification of a personal data breach to the supervisory authority).
Decision:	Administrative fine, Violation identified.
Key words:	Administrative fine, Data minimisation, Data retention, Data security, Transparency, Payment data, Lawfulness of processing, Clients, Data processing agreement, Sensitive data, Consent, Retention time

Summary of the Decision

Origin of the case

The controller is a company registered in France. It provides online clairvoyance readings to its customers through chat or on the phone. The LSA opened an investigation following a report in the press that the controller had been subject to a data breach. More specifically, the LSA carried out an online investigation, an onsite audit and also asked the controller to respond to specific questions and requests for information.

Findings

The LSA found that the controller breached many GDPR provisions.

First, the LSA found that the controller breached the data minimisation principle under **Article 5(1)(c) GDPR** because it collected excessive personal data for the applicable purposes. More specifically, the controller was systematically recording all the phone calls between on the one hand, its prospects and call agents, and on the other hand between its fortune-tellers and customers. The controller failed to justify the necessity to record all calls and the LSA considered that there were less intrusive means to achieve the different purposes identified by the controller. In addition, during the calls that were recorded, the customers shared their payment card details. The controller did not implement any specific measures to pause the recording of the phone calls during this data disclosure even though such data was not relevant for the purposes identified by the controller.

Secondly, the LSA found that the controller breached the storage limitation principle under **Article 5(1)(e) GDPR**, as it retained customer data for an excessive period after the end of the applicable contractual relationship. During the investigation, the controller's active database included personal data relating to customers who had not had a clairvoyance reading in more than three years (and sometimes in more than five years) without the controller justifying that customers still have credit.

In addition, the LSA found that the controller did not rely on a legal basis under **Article 6 GDPR**. The controller retained payment card information of its customers after the completion of transactions to facilitate the purchase of additional credit without their prior consent. According to the LSA, this processing activity cannot rely on the necessity to perform the contract.

Furthermore, the LSA found that the controller breached **Article 9 GDPR**. When providing clairvoyance services, the controller collected and processed customers' sensitive data (i.e. data concerning health and data about sexual orientation) without the data subjects' prior and explicit consent. The LSA rejected the controller's argument whereby spontaneously contacting a fortune-teller and disclosing special categories of personal data during the call with the latter amount to explicit consent on the part of the customers. To obtain "informed" consent, data subjects must first be provided with specific information regarding this processing activity, which was not the case in this context.

The LSA also found that the controller breached its transparency obligations under **Articles 12 and 13 GDPR**. The information provided by the controller was not easily accessible given that users had to actively search for it. More specifically, the information was not provided directly on the registration online page and it was included in a document not identified as such as relating to data protection, but in the standard terms and conditions. The LSA also considered that the information provided to users was incomplete as it did not include all the information required by Article 13 GDPR.

In addition, the LSA found that the controller breached **Article 28 GDPR** when contracting with processors. The data processing agreements in place were not all signed by the parties and did not include all the mandatory information set out under Article 28(3) GDPR. As a result, the LSA considered that the contractual safeguards were not sufficient.

Furthermore, the LSA found that the controller breached **Article 32 GDPR** for not having implemented basic security measures. The controller implemented insufficiently robust passwords for user accounts (for its customers as well as its employees) and did not secure access to its customer website using the http protocol instead of the https protocol. Lastly, the controller also used a bank data encryption mechanism that had vulnerabilities.

Lastly, the LSA found that the controller breached **Article 33 GDPR**. The controller was aware of the occurrence of a data breach and recorded the breach in its data breach internal register. However, it failed to notify the breach to the LSA. According to the LSA, at the date of the internal investigation, the controller had a reasonable degree of certainty that there was a data breach causing a risk to data subjects' rights and freedoms, especially given the duration of the breach (i.e., two months and four days) and the potential high number of data subjects. The obligation to notify the competent authority applies even if the breach was caused by an error that could be attributed to the processor.

Decision

The LSA imposed on the controller an administrative fine of 120,000 euros for the infringement of Articles 5(1)(c) and (e), 6, 9, 12, 13, 28, 32 and 33 GDPR. The LSA also decided to publish the final decision on its website and on the Légifrance website for two years, after which the controller will not be identifiable anymore.

To set the amount of the administrative fine, the LSA took into account the particularly high number of GDPR infringements, the fact that it involved special categories of personal data and the high number of data subjects. It also took into account the financial situation of the controller and the fact that it employed few employees.

Deliberation of Restricted Committee no. SAN-2023-009 of 15 June 2023 concerning

[REDACTED]

The *Commission nationale de l'informatique et des libertés* (CNIL), meeting in its Restricted Committee composed of Mr Alexandre Linden, Chairman, Ms Christine Maugué and Messrs Alain Dru and Bertrand du Marais, members;

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 on the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 et seq.;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to deliberation No. 2013-175 of 4 July 2013 concerning adoption of the CNIL's internal regulations;

Having regard to Decision No. 2020-005C of 27 December 2019 of CNIL's Chair to instruct the general secretary to carry out, or have a third party carry out, an assignment to verify the processing implemented by the company [REDACTED] or on its behalf, in any location that may be concerned by the implementation of said processing;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 23 June 2021;

Having regard to the report of François Pellegrini, commissioner and rapporteur, notified to [REDACTED] on 03 August 2022;

Having regard to the written observations made by the counsel of [REDACTED] on 31 October 2022;

Having regard to the rapporteur's response to these comments notified to [REDACTED] on 7 December 2022;

Having regard to the new written observations made by the counsel of [REDACTED], received on 30 January 2023;

Having regard to the oral observations made during the Restricted Committee session;

Having regard to the other documents in the file;

The following were present during the Restricted Committee session on 16 March 2023:

- Mr François Pellegrini, commissioner, his report having been read;

In the capacity of representatives of [REDACTED]:

- [REDACTED]

[REDACTED]

By videoconference: [REDACTED]
[REDACTED]

[REDACTED] having spoken last;

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. Founded in [REDACTED] in France, [REDACTED] (hereinafter the “Company”) specialises in the display of targeted advertising on the web. In 2022, the [REDACTED] employed approximately [REDACTED] employees and had a total turnover of approximately [REDACTED] for a net profit of approximately [REDACTED]
2. The company implements so-called “advertising retargeting” data processing, which consists of tracking Internet users’ browsing habits to display personalised advertising to them, using cookies placed in users’ terminals.
3. On 8 November 2018, the *Commission nationale de l'informatique et des libertés* data protection authority (hereinafter “the CNIL” or “the Commission”) received a complaint sent by the “Privacy International” association, which emphasised in particular that the company had not been processing the data of Internet users in accordance with the principles set out in Article 5(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 (hereinafter “the GDPR”).
4. On 4 December 2018, the CNIL received a complaint sent by the “None of Your Business” association (hereinafter “NOYB”) commissioned by [REDACTED], criticising the formalities imposed by the company from which he had wished to withdraw his consent and object to the processing of his data (hereinafter “the complainant”). The complainant stated that, despite having sent an email to this effect to the company, it had redirected him to various online procedures devoted to the exercise of rights.
5. On 14 January 2019, in accordance with Article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by the company, a competence derived by CNIL from the fact that the company’s main establishment is located in France.
6. After exchanges between data protection authorities, it turned out that all European authorities are covered within the meaning of Article 4(22) of the GDPR.
7. As part of the investigation of the complaint lodged by NOYB, CNIL questioned the company on the follow-up to the complainant’s requests. This investigation led to an exchange of letters between CNIL and the company, dated 27 March, 29 April, 9 September, 9 October, 27 December 2019 and 17 February 2020. A meeting was also held on 17 January 2020.

8. Further to this instruction, and pursuant to Decision No. 2020-005C of 27 December 2019 of the Chair of the Commission, a CNIL delegation carried out several checks on the company in order to verify compliance with the provisions of Law No. 78-17 of 6 January 1978 as amended on data processing, files and freedoms (hereinafter “the French Data Protection Act” or “Law of 6 January 1978”) and the GDPR.
9. On 29 January 2020, the delegation sent a questionnaire to the Company, to which the company replied on 27 March 2020, concerning its organisation, the personal data processing that it implements, its qualification as a data controller, its relations with its customers and partners, and its management of requests to exercise rights.
10. On 16 and 17 September 2020, the delegation conducted an on-site investigation at the company’s premises, during which it carried out audits on the website of two partners of the company. The delegation also checked the follow-up to the complainant’s request to exercise his rights and obtained information on how to implement the right to withdraw consent and the right to erasure. The onsite investigation led to the production of two reports, no. 2020-005/1 and no. 2020-005/2, supplied to the company on 30 September 2020.
11. On 13 October 2020, using a list provided by the company of the hundred websites from which it collects the most data, the delegation conducted an online audit on several of these sites to verify such aspects as the procedures for placing the [REDACTED] cookie on user devices and the mechanism implemented to obtain their consent. The online inspection led to the production of report no. 2020-005/3, supplied to the company on 14 October 2020.
12. On 23 June 2021, on the basis of Article 22 of the Act of 6 January 1978, the Chair of the Commission appointed Mr François Pellegrini as rapporteur for the purpose of investigating these elements.
13. On 9 June 2022, the rapporteur sent an additional request to the company, requesting in particular the latest versions of the general terms and conditions of use of the [REDACTED] services, as well as a recent sample of contracts entered into by the company with its partners. The company responded on 17 June 2022.
14. On 3 August 2022, at the end of his investigation, the rapporteur notified the company of a report detailing the breaches of Articles 7, 12, 13, 15, 17 and 26 of the GDPR, which he considered established in this case.
15. This report made a recommendation to the Restricted Committee of the Commission to impose an administrative fine against the company of an amount of no less than sixty million euros. It also proposed that this decision be made public and that the company no longer be identifiable by name upon expiry of a period of two years following its publication.
16. On 31 October 2022, the company submitted observations in response to the rapporteur’s report.
17. On 7 December 2022, the rapporteur replied to the company’s observations.
18. On 30 January 2023, the company submitted further observations in response to those of the rapporteur.

19. In a letter dated 21 February 2023, the rapporteur informed the company's counsel that the investigation was closed, pursuant to Article 40, III, decree no. 2019-536 of 29 May 2019 implementing the French Data Protection Act.
20. The rapporteur and the company presented oral observations at the Restricted Committee session, which took place on 16 March 2023.

II. Reasons for the decision

A. On the European cooperation procedure

21. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 16 May 2023.
22. As of 13 June 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

B. On the processing in question, the qualification of personal data and the liability for processing.

1. On the processing in question for the purpose of displaying personalised advertising

23. Article 4(2) of the GDPR defines processing as "*any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, preservation, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction.*"
24. In this case, the **Restricted Committee** notes that the company implements data processing called "advertising retargeting" for the purposes of displaying personalised advertising (hereinafter the "processing in question").
25. In practical terms, the company collects browsing data from Internet users through cookies that are stored on their terminals when they visit one of their [REDACTED] partners' websites, including publishers and advertisers. When an Internet user visits a partner's website, the company stores a cookie on the device their browser is running on. This is assigned a unique identifier, called [REDACTED] ID, which will enable it to recognise him/her during future visits to the partner's other sites.
26. So when an Internet user visits a partner advertiser's website, the company records in its database the internet user's actions via the cookie (for example, visiting the home page, connecting to a user account, clicking on a "product" page, adding an item to the shopping basket).
27. Then, when the user visits the website of a partner publisher, the publisher sends a request to the company for information such as the size of the advertising insert, the nature of the publisher website and an identifier allowing the company to recognise the user.

28. The company then uses its data processing technologies to determine which advertising would be most relevant to display to the Internet user according to their browsing habits and the products or services that may be of interest to them. Based on this analysis, the company then engages in “real-time bidding” (RTB) for displaying an ad on the publisher’s advertising space. If the company wins the bid, an advertiser’s advertising banner is displayed in the insert available on the publisher’s website.
29. In this way, acting as an intermediary between advertisers and website publishers, the company not only helps advertisers to reach their target audience with more relevant advertising, but also helps publishers to promote their advertising spaces.
30. The Restricted Committee notes that the company has acknowledged implementing the processing described in the preceding paragraphs.

2. On the qualification of the data processed by [REDACTED] as personal data

31. Article 4(1) GDPR defines personal data as “*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.*”
32. Recital 30 of the GDPR, which is part of well-established case law of the Court of Justice of the European Union (CJEU, 24 Nov. 2011, *Scarlet Extended SA C 70/10*, pt. 51 and 19 Oct. 2016, *Breyer*, C-582/14) provides that an online identifier associated with a natural person, such as an IP address or a login cookie, may “*leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*”
33. In its aforementioned *Breyer* judgement, handed down under Directive 95/46/EC, the CJEU stressed the importance of a case-law approach to whether a data item was an “identifier” or not, rather than a general position based on principle. It stated that, in order to determine whether an individual is identifiable, account should be taken of all the means likely to be reasonably used, either by the data controller or by another individual, to identify that individual.
34. **The rapporteur** is of the view that the company processes personal data, taking into account that – in view of the number and diversity of the data collected and the fact that they are all linked to an identifier – it is possible, with reasonable means, to re-identify the natural persons to whom such data relates.
35. **The company** maintains that it processes “*browsing events*”, which are pseudonymised technical data that do not enable it to directly identify the Internet users with which they are associated. It argues that it is only required to recognise the identity of an individual in the event of a request for a right of access where they can match the [REDACTED] cookie identifier ([REDACTED] ID) and the identity of the individual. Outside of such a hypothesis, it considers that the risk of re-identification is very low and produces simulations on this point carried out by service providers.
36. It concludes that since it only processes pseudonymised data, any possible breaches it may have committed have had a very limited impact on the data subjects, which the Restricted Committee should take into account in its assessment.

37. **The Restricted Committee** points out that only genuine anonymisation of the data processed, causing the data to lose their “personal” nature – i.e., without the possibility of re-identifying the natural person to which they relate – would exempt the processing from all the requirements of the GDPR.
38. In this specific case, the Restricted Committee notes that although the company maintains that it does not process anonymised data, it claims to process only pseudonymised data with a very low risk of re-identification.
39. The Restricted Committee also notes that the [REDACTED] ID cookie identifier, assigned by the company by means of the cookies it places, is intended to distinguish each individual whose data it collects, and that very many items of information intended to enrich the web user’s advertising profile are associated with this identifier, including:
- data related to the identification of the individual: geographical location from IP address, [REDACTED] user ID, device identifier, partner-provided identifiers, email address in hashed form provided by the partners;
 - data related to the individual’s activity, which corresponds to the tracking of the web user’s browsing history through the sites visited, the products viewed or added to the basket, and the act of purchasing. This also includes any interactions the user has with the advertisements presented to them (did the user click on the banner? did they make a purchase?);
 - data derived or inferred from the above information in order to be able to offer the user the most relevant products, taking into account their interests.
40. The Restricted Committee thus notes that although the company does not directly possess the identity of the natural persons to which the devices on which cookies are registered are linked, re-identification may be facilitated by the fact that, in certain cases, the company collects – in addition to data related to browsing events – other data facilitating re-identification, such as the e-mail addresses of the individuals whose browsing journeys have been from within an authenticated (or “logged”) environment in hashed form, the identifiers corresponding to them generated by other players, the IP address in hashed form and the user agent of the device used.
41. Therefore, once the company is able to re-identify individuals by reasonable means, the processed data retain a personal character, within the meaning of Article 4.1 of the GDPR.
42. It follows that the GDPR is applicable and that, having regard to what has been indicated above, the company is a data controller for the processing in question.
- C. On the failure to comply with the requirement of demonstrating that the data subject has given his/her consent;**
43. Pursuant to Article 6(1) of the GDPR: “*Processing shall be lawful only if and to the extent that at least one of the following applies:*
- a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
- b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

- c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.”

44. Article 4(11) of the GDPR defines consent 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”.
45. Article 7(1) of the GDPR relating to the conditions applicable to consent provides that: “where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.”
46. **The rapporteur** considers that the company has not put in place any measures to ensure that the personal data it processes are only data for which valid consent has been collected from the individual. It notes that of the websites audited by the CNIL, more than half of the websites published by its partners did not obtain valid consent and that the company had not implemented an audit mechanism for its partners.
47. **The company**, citing the *Fashion ID* judgement (CJEU, 29 July 2019, C 40/17), argues that its partners, who have the capacity of joint data controllers, remain the best placed to collect the consent of the data subjects in that the [REDACTED] cookie is placed on the devices of Internet users when browsing their website.
48. The company adds that in this respect, the various agreements entered into with its partners pursuant to Article 26 of the GDPR (in particular the aforementioned General Terms and Conditions of Service and its Data Protection Agreement) provide that this obligation lies with them. It considers that this contractual distribution is sufficient to ensure compliance with this obligation, which is binding on its partners under the principle of binding force of contracts.
49. It argues that there is no evidence that the practices observed on the twelve websites visited by the audit delegation are representative of the state of compliance of its [REDACTED] partners.
50. Although it claims that it has no obligation itself to ensure that its partners have validly obtained the consent of the data subjects, the company nevertheless points out that it does not hesitate to terminate contracts signed with parties who do not comply with their obligations in terms of obtaining the consent of Internet users.

51. It adds that it has implemented other auditing mechanisms, such as a strategy for auditing its partners which, as at 31 October 2022, has verified the state of compliance of nearly [REDACTED] of its partners, as well as a so-called “*Know Your Client*” process by which it checks the compliance of its future partners with several regulatory requirements (presence of a cookie banner and privacy policy) prior to entering into a service contract with them. Finally, it states that it has terminated a contract it had with one of its partners which had been audited by the CNIL delegation, and has sent a warning to another partner who did not comply with the regulations applicable to the collection of consent from Internet users.
52. **The Restricted Committee** points out that in the case of joint liability, Article 26 of the GDPR obliges joint data controllers to ensure, through an agreement, that they mutually comply with the GDPR and, in particular, that they work together to determine the best way to respond to the rights of data subjects, depending on the nature of the processing and their respective responsibility for such processing.
53. It points out that in points 167 and 168 of its guidelines 07/2020 on the concepts of data controller and data processor in the GDPR, the European Data Protection Board (EDPB) considers that in case of joint responsibility, “*both data controllers are always required to ensure that both have a legal basis for the processing*” and that they “*may have a certain degree of flexibility in the division and allocation of responsibilities between them, provided that they ensure full compliance with the requirements of the GDPR with regard to the specific processing*”.
54. Firstly, with regard to the respective roles and obligations of [REDACTED] and the partner sites, the Restricted Committee notes that as part of its processing for the purpose of displaying personalised advertising, the company processes the personal data of Internet users visiting the websites of its partners which are collected in advance through the [REDACTED] cookie.
55. It also notes that the company and the websites of its partners from which the [REDACTED] cookie is deposited on the devices of Internet users are jointly responsible for the operations of depositing the [REDACTED] cookie and for the collection of data from Internet users carried out using this cookie.
56. With regard to the legal framework applicable to these various processing operations, the Restricted Committee recalls that if the storage of the [REDACTED] cookie on the device of the user visiting a partner’s website, enabling the company to assign a unique identifier to that user, is subject to the provisions of Article 5(3) of Directive 2002/58/ EC of the European Parliament and of the Council of 12 July 2002 on the protection of privacy in the electronic communications sector (hereinafter the ““ePrivacy’ Directive”), transposed into French law in Article 82 of the French Data Protection Act, the subsequent processing for advertising purposes, which is carried out from the personal data collected through this cookie, is subject to the provisions of the GDPR.
57. With regard to the legal basis applicable to these various processing operations, the Restricted Committee first points out that under the “ePrivacy” Directive, operations for reading or writing information in a user’s device cannot be implemented without the user’s prior consent.
58. It then notes, with regard to the processing in question, that the company stated to the auditing delegation in its response to the questionnaire of 29 January 2020 that: “*all processing that we carry out in connection with our advertising services in Europe is based on user consent.*” Furthermore, the company’s processing privacy policy also mentions consent as the legal grounds applicable for the purposes of displaying personalised advertising, whether targeted or contextual.

59. The Restricted Committee notes that, according to a consistent position of the CNIL, the overlap between the rules of the “ePrivacy” Directive and the GDPR allows the publisher of the website from which the cookie is saved to collect the consent necessary for saving the cookie at the same time necessary for the subsequent processing implemented from the data collected by this cookie.
60. Specifically, it notes, in this case, that the company has made an arrangement with its partners such that the general conditions of use of the [REDACTED] services, to which the partners of the company have subscribed, specify that it is the responsibility of the partner to obtain the consent of the data subject for the subsequent processing carried out on the basis of the data collected by this cookie.
61. However, the Restricted Committee considers that the mere fact that the collection of the consent of Internet users for the implementation of the processing in question is the responsibility of the partners does not exempt the company from its obligation, pursuant to Article 7 of the GDPR, to be able to demonstrate that the data subject has given his/her consent.
62. This dual-liability regime ensures that at all stages of the processing of data collected for a user’s browsing on one of the company’s partner sites, each joint data controller complies with the provisions incumbent upon it: for partners, those relating to the storage and reading of the [REDACTED] cookie on the user’s device and, for the company, those provisions relating to subsequent processing carried out from the data collected by this cookie.
63. Specifically, the data subjects are required to benefit from the protection offered by the legislation in force to which they are entitled throughout their browsing and, in particular, that their data are processed by the company only if they have previously and validly consented to it.
64. In addition, the company’s core activity is to transform raw browsing data into valuable information that it uses. The fact that the company plays a central role in the advertising ecosystem is all the more reason why it must be able to ensure that the processing in question complies with the regulations in force.
65. Finally, the Restricted Committee notes that the *Fashion ID* judgement, referred to by the company, deals with the question of whether it was the website manager (*Fashion ID*) or the publisher of the cookie (Facebook) who was responsible for obtaining the consent of the data subjects before filing the cookie published by Facebook and that it was handed down under Directive 95/46/EC on data protection.
66. Insofar as the European legislator has intended to strengthen individual rights and stakeholder accountability by establishing, in particular, the obligation for the data controller to be able to demonstrate that the individual whose data it processes has actually given his/her consent, pursuant to Article 7(1) of the GDPR, the Restricted Committee considers that the reference to the *Fashion ID* judgement is not relevant in this case.
67. Secondly, the Restricted Committee notes that in connection with the online checks carried out during the on-site investigations of 16 September 2020 and during the online audit of 13 October 2020, the delegation found that on seven company partner websites, a [REDACTED] cookie had been placed on the device used on this occasion, at the time of its arrival on the home page without it having carried out the slightest action; whereas, at the time of these findings, the CNIL had already had been prompted to issue a reminder that such practices directly contradicted the provisions of the French Data Protection Act applicable to cookies.

68. The Restricted Committee also notes that in three cases, the website being visited did not allow the user to refuse cookies other than by configuring his/her browser, which does not constitute a mechanism for refusing valid consent, while in two cases, a [REDACTED] cookie was placed after the delegation had expressed its refusal to such storage.
69. In addition, as part of the on-site investigations of 16 September 2020, the delegation noted that the two websites visited did not contain any mechanism for obtaining consent to the deposit of cookies, such as a button or a box to be ticked. Several events related to the browsing of these two sites have been recorded in the company's database, such as visiting the pages of products sold by the company's partners.
70. It emerges from all these checks that the absence of valid consent was noted by the delegation on almost one in every two sites visited. Yet the Restricted Committee also notes that details of nine of the twelve sites visited by CNIL staff were provided by the company itself, as those generating the largest amount of data collected in its database.
71. While it is true that the audit procedure did not permit verification of all the sites of the company's [REDACTED] partners, the Restricted Committee considers that it can reasonably be inferred from the aforementioned findings that as of the date of the checks, the company processed a large volume of browsing data for which Internet users had not given valid consent.
72. Thirdly, the Restricted Committee notes that at the date of the initiation of the audit procedure, the company had not implemented any satisfactory measures to suggest that it was in compliance with the requirements of Article 7(1) of the GDPR.
73. Thus, the Restricted Committee notes that at the beginning of the audit procedure, in response to the delegation's question regarding the measures put in place by the company to ensure the validity of the consent, in the event that it had to delegate the collection of this consent to a third party, the company had simply reproduced a reference to its general terms and conditions of use, in their applicable version of May 2016, according to which the company required its partners, "*where the law so provides*", to ensure that the privacy policy of their website included "*information and choice mechanisms in accordance with applicable laws and regulations*".
74. It is the view of the Restricted Committee that such a clause did not, on its own, ensure the existence of valid consent and that, at the very least, a supplementary clause needed to be added to specify that the body collecting consent must make proof of consent available to the other party, so that all data controllers wishing to rely on it could actually refer to it.
75. In this case, the Restricted Committee notes that on the date of commencement of the audit procedure, this clause was not only not supplemented by a specific clause on proof of consent, but also that the company had additionally admitted that it had never terminated a contract due to a partner's failure to comply with its contractual obligations, nor implemented any other auditing measures on its partners.
76. In relation to this, the Restricted Committee notes that the various measures referred to by the company were progressively implemented only from 2020, after the initiation of the audit procedure initiated in January 2020.

77. The Restricted Committee thus takes note of the company's audit campaign with its partners since 2020 and the fact that the company has also terminated the contract it had with one such partner who did not comply with its obligations in terms of cookies.
78. It similarly notes that in subsequent versions of its general conditions of use, the company has inserted a clause relating to proof of consent that the partner undertakes to "*provide promptly to [REDACTED], upon request and at any time, proof that the consent of the data subject has been obtained by the partner*".
79. In light of this information, the Restricted Committee considers that the company has complied with the requirements of Article 7(1) of the GDPR.
80. It nevertheless points out that this late achievement of compliance does not alter the fact that the company has processed the personal data of Internet users without being able to demonstrate that they validly consented to the processing whose purpose is to display personalised advertising, in breach of Article 7(1) of the GDPR.

D. On the violation of information and transparency obligations

81. Article 12(1) of the GDPR states that: "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.*"
82. According to Article 13 of the GDPR, the data controller must provide the data subject with the following information:
"a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
b) the contact details of the data protection officer, where applicable;
c) the purposes of the processing for which the personal data are intended, as well as the legal grounds for the processing;
d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the data controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any; and
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;".
83. **In this case, the rapporteur** maintains that the information provided by the company to the data subjects was not complete in that it did not contain all the purposes relating to the processing in question in the version of its confidentiality policy applicable on the date of the findings, including the purpose relating to the improvement of its technologies.
84. The rapporteur also criticises the company for a lack of clarity as to the legal grounds for consent applicable to the processing; the company specifies that this differs from country to country, and according to the purposes implemented on the basis of the legitimate interest.

85. **The company** responds that it has updated its privacy policy.
86. It contests this first complaint in any case, maintaining that it did not have to specify the purpose of improving its technologies since, in its view, this purpose includes technical elements that contribute to the same overall purpose as the display of personalised advertisements.
87. On the second objection, it argues that the possible ambiguities criticised by the rapporteur have never prevented the data subjects from exercising their rights.
88. In its second observations, the company argues that it cannot be accused of any breach of its obligations under Article 13 of the GDPR insofar as it only collects data indirectly.
89. **The Restricted Committee** points out, firstly, that the GDPR makes a distinction over the regime governing the obligation to inform which is imposed on the data controller according to the nature of the data collection: the data controller is subject to the provisions of Article 13 of the GDPR when the data are collected directly from the data subject, and to the provisions of Article 14 of the GDPR otherwise.
90. It adds that in point 26 of its guidelines of 29 November 2017 on transparency, in their revised version of 11 April 2018, the EDPB points out that Article 13 of the GDPR also applies when the data is collected by the data controller “*by observation*”, i.e. when the data controller collects the data via the use of sensors of any kind.
91. The Restricted Committee notes that the French Conseil d’Etat adopted the same interpretation in a decision handed down before the entry into force of the GDPR, considering that the fact that the collection does not require any intervention on the part of the data subjects had no impact on the direct nature of this collection (Conseil d’Etat, 10th - 9th chambers combined, 8 February 2017, *JCDecaux*, No. 393714).
92. In this case, the Restricted Committee notes that the data is indeed collected by the company directly from the Internet user, as when that user browses the website of a partner of the company, the requests of the [REDACTED] cookie enabling the partner to identify that an Internet user is visiting home page, log into an account or click on a “product” page, are sent directly to its servers, without transiting via another data controller.
93. As the data is collected from individuals, the Restricted Committee concludes that Article 13 of the GDPR applies to the company.
94. Secondly, the Restricted Committee notes that the general terms and conditions of use of the [REDACTED] services provide that the company’s partners must incorporate a personal data protection policy, containing a link to [REDACTED]’s privacy policy, into their website.
95. It notes that the “*Legal grounds for data processing*” section of the company’s privacy policy, in its version applicable on the date of the findings, stated that: “[REDACTED]’s processing operations comply with the regulations in force, in countries requiring the consent of users for the use of cookies or any other similar technology. This consent is collected on the Advertisers’ and Publishers’ websites and mobile applications.”

96. Furthermore, it was also stated in the same section that: ‘[REDACTED] believes that it has a legitimate interest in processing your data for the purposes expressed in this privacy policy, in particular to:
- adhere to the commercial agreements made with our clients and partners;
 - enable our Advertisers to promote their products and services;
 - enable our Publishers to fund their activities.’
97. The Restricted Committee considers, firstly, that the first wording creates uncertainty as to the legal basis for processing, in that it does not make it clear to Internet users located within the European Union that the processing of their data is based on their consent.
98. Next, it states its belief that the purposes announced by the company are expressed in vague and broad terms that do not give users a clear understanding of which personal data are being used for what purposes. Furthermore, the Restricted Committee considers it contradictory to state that the purposes relating to the promotion of advertisers’ products and the financing of publishers’ activities are based on the legal basis of legitimate interest, when in fact these purposes are directly linked to the processing of displayed personalised advertising, which, as the company itself acknowledges, is based on the legal grounds of the consent of Internet users. The Restricted Committee adds that such a vague and contradictory description of the purposes pursued on the basis of legitimate interest is likely to hamper the exercise by data subjects of their right to object, which is intrinsically linked to the quality of the information provided.
99. The Restricted Committee notes that the company has responded to these shortcomings in the new version of its privacy policy; it now specifies that consent applies to individuals residing in the European Economic Area and includes a table summarising all the purposes of its processing, including those based on the legal grounds of legitimate interest, which includes a detailed description of these purposes and the categories of data concerned. The Restricted Committee notes that the company has also removed the contradiction noted above.
100. Thirdly, the Restricted Committee notes that the “*Purpose of the processing of personal data*” section of the company’s privacy policy, in its version applicable on the date of the findings, contained only the following line: “[REDACTED] processes your personal data to display personalised ads”.
101. However, during the on-site investigations of 16 and 17 September 2020, the company specified to the delegation that the processing also allowed it “*to optimise the responses to be given to auctions and the selection of items to be presented in an advertisement, and to suggest the best layout for this banner*”.
102. While the Restricted Committee admits that certain technical operations described by the company directly contribute to the main purpose of displaying personalised advertising, it is of the opinion that by contrast, others serve a separate purpose.
103. Indeed, the company uses the data collected through cookies in order to improve its own technologies (purpose called “machine learning”, mobilising the data collected by the company to auto-configure algorithm-driven targeting processing operations). Thus, the main objective of this subsequent processing is to improve the overall effectiveness of the advertising targeting carried out by [REDACTED]. This is therefore a separate purpose, which must be brought to the attention of the data subjects.

104. The Restricted Committee also notes that the new version of its privacy policy, posted online on 4 November 2022, clearly distinguishes, within the “*Use of your data*” section, (a) the purpose of “*display of personalised advertising*” and (b) the purpose of “*training models*”, defined as making it possible to “*improve the performance of [REDACTED]’s advertising operations*”.
105. The result of the above is that by not providing data subjects with all the information required, by using insufficiently clear and precise terms, and by presenting erroneous legal grounds for the processing operations, the company has failed to fulfil its transparency and information obligations under Articles 12 and 13 of the GDPR. However, the Restricted Committee takes note of the fact that the company was compliant during these proceedings.

E. On the violation of the obligation to uphold the right of access of data subjects to their personal data

106. Article 12(1) of the GDPR states that: “*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language*”.
107. Article 15(1) of the GDPR states 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 [...]*”.
108. **In this case**, as part of the investigations carried out by the CNIL, the company provided the delegation with three examples of responses sent to data subjects who made access requests.
109. It emerges from this that when an individual exercised his right of access with the company, it sent that individual the data extracted from the following three tables:
- the “*Advertiser_advert*” table, which stores all data related to the advertiser’s events;
 - the “*Banner_display*” table, which stores all the data necessary to enable an advertisement to be displayed to the user (e.g.: the user’s country, advertiser-related data or the version of the operating system of the user’s device);
 - the “*Click_cas*” table, which stores all the data related to a user’s interactions with the advertising banners.
110. **The rapporteur** is of the view that the company only partially responded to requests for access rights made to it, since it did not supply the data contained in three other tables:
- the “*Usermatching*” table, which contains the information enabling [REDACTED] identifiers to be reconciled (in the event that the same user uses several devices) in a “deterministic” manner (the company relies on information provided by its partners, such as a loyalty card number, an Apple or Android identifier, and/or an e-mail address in hashed form to create a link between two [REDACTED] identifiers);
 - the “*bc_tcp_timestamp*” table, which contains information enabling the reconciliation of identifiers in a “probabilistic” way (the company applies a prediction model from the data linked to two identifiers that it believes correspond to the same user);
 - the “*Bid_request*” table, which contains information related to events related to the online auction protocol.

111. It is also of the view that the provided information was not intelligible to the user, as the company merely provided a summary description of the goal of each table, yet did not provide explanations on the goal of each of the columns in these tables, nor on their content.
112. **The company** argues that its procedures in the event of requests made under the right of access comply with the requirements of Article 15 of the GDPR. More specifically, it returns to each of the three tables listed by the rapporteur and explains why, in the event of a request for access, it did not communicate the data they contained.
113. With regard to the “*Usermatching*” table, the company argues that it only contains data enabling the reconciliation of the [REDACTED] identifier with other identifiers, but that it nevertheless undertook to provide these data as part of its responses to access requests from November 2022.
114. With regard to the “*bc_tcp_timestamp*” table, the company argues that this table, which is based on a probabilistic method, may potentially reconcile two distinct individuals, so that the communication of data could potentially harm the rights and interests of third parties in the event that the data relating to another individual are communicated to the originator of the access request. For this reason, it excluded this table from its responses to access requests.
115. With regard to the “*bid_request*” table, the company argues that it contains approximately 400 fields relating to auction requests, so that these are essentially technical data and that the remaining data are identical to those appearing in the “*Banner_display*” table already provided by the Company. However, it specifies that it had committed to providing all of these data as part of its responses to access requests by March 2023, the time required to implement an action plan that will allow it to extract these data by profile.
116. With regard to the intelligibility of the information provided to data subjects, it states that it has supplemented the explanations with a table that, for each table, lists the nature of the data processed, and provides a description and examples of data, which it sends in its response to access requests.
117. **The Restricted Committee** takes note of the explanations given by the company for the “*bc_tcp_timestamp*” table and in fact considers that the company was not required to provide the data of this table, insofar as they may concern several individuals without the company being able to identify with certainty which data concerns exclusively the individual making the request.
118. With regard to the “*Usermatching*” and “*bid_request*” tables, it is of the opinion that the information presented and produced by the company now enable users to better understand the information sent to them.
119. The Restricted Committee notes, however, that the explanations provided by the company do not, on the date of the findings, justify the non-communication of the data contained in these two tables, whereas it is not disputed that these tables contain personal data which may be combined with other data recorded by the company and, in particular, with the identifier assigned to each Internet user.
120. It adds that it emerges from these same findings that, in its response to requests for access rights, the company explained the objective of each table in a brief sentence, and invited users to send an email for more information. By not automatically providing information on the purpose and

content of each of the columns in these tables, the company left users uncertain as to the nature of the processed data concerning them.

121. The result of the above is that, by not communicating all the personal data of the individuals exercising their right of access to it and by not officially providing them with documentation enabling them to understand the data supplied to them, the company failed to fulfil its obligations under Articles 12 and 15 of the GDPR.

F. On the violation of the obligation to uphold the right to withdraw consent and to erasure of data

122. Article 7(3) of the GDPR states that: “*The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as simple to withdraw as to give consent.*”
123. Under 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 following grounds applies:*
- [...]
- 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*
- [...]
- d) *the personal data have been unlawfully processed*
- [...].
124. In this case, exchanges took place between the CNIL and the company following the receipt of [REDACTED]’ complaint concerning his individual situation but also, more generally, the procedures implemented by the company to respond to requests to exercise the rights of individuals. The company stated that it had improved the measures put in place, in particular to make effective the right to withdraw consent and the right to erasure of data.
125. The outcome of investigations subsequent to these exchanges and the introduction of the measures announced by the company is that data subjects who wished to withdraw their consent to the processing of their data by the company, or who exercised their right of erasure, could do so by clicking the “*Disable [REDACTED] services*” button accessible in the company’s privacy policy found at “[REDACTED].com”. The company specified that when an individual clicks on this button, an “*opt-out cookie*” is placed in the individual’s browser, thus preventing the subsequent placement of [REDACTED] cookies and the display of personalised advertisements.
126. The company stated that the deactivation of the [REDACTED] services, i.e. the act of no longer displaying personalised advertising to the individual, could also be effected by using the platforms made available by professional associations representing the sector, such as the “*YourOnlineChoices*” platform.
127. During the on-site investigations of 17 September 2020, the delegation noted that the company was no longer tracking the user ID assigned to [REDACTED] in its databases. During the same audit,

the company stated that the opt-out procedure for its services no longer enabled it “*to link the user ID in question to the user’s browser, so that no advertising will be offered to this identifier*”, without having the effect of removing from its tables the user ID originating the objection or erasure request. The company added that: “*in the event that a user identifier has been disabled, it will no longer be possible to match events related to that identifier with any other identifiers related to that user*”. Lastly, the company stated that it could re-use the [REDACTED] user ID, and the events related to the request for deactivation, for the purpose of improving its technologies.

128. **The rapporteur** is of the view that the company has not met the requirements of Article 17 of the GDPR since it is not removing the individual’s identifier or deleting the linked browsing events, despite the fact that the processing of [REDACTED]’ complaint demonstrates that it is indeed able to effectively erase the data it processes.
129. **The company** argues that it is not required to make such a deletion if it has a legitimate interest in retaining and processing the data of individuals who have made a request for erasure for the following six purposes: reconciliation of sales/allocation, prevention of fraud / fight against fraud, training of models, invoicing, reporting and incident resolution.
130. For this reason, it considers itself justified in not effectively deleting this data as long as the pursuit of these other purposes based on the legitimate interest justifies their retention. For each of these six purposes, the company has produced a study demonstrating the relevance of using this legal basis.
131. Specifically with regard to the purpose of training models, the company is of the view that this allows data subjects to receive even more personalised advertisements, which is also in their interest. It adds that the CNIL has already recognised, in sanction deliberation no. 2013-420 of 3 January 2014 and in a decision MED-2017-075 of 27 November 2017, that “*the improvement of services*” could be considered as a legitimate interest for a data controller.
132. **The Restricted Committee** notes that when it responds to a request for erasure, the company does no more than halt the display of personalised advertisements on the device of the individual making the request, without effectively deleting the data relating to that individual.
133. The Restricted Committee notes that the company claims that it cannot perform such erasure on the grounds that it requires the data collected during its advertising targeting processing, based on consent, to carry out six other purposes which, according to the latter, are based on the legal grounds of legitimate interest.
134. However, without it being necessary to rule on the suitability of the legitimate interest as legal grounds for each of the six purposes put forward by the company, the Restricted Committee considers that, in cases where the company was in any event unable to ensure that the individual originating the request had validly consented to the processing of his/her data by the company, the company could not continue to process the data of this individual for subsequent purposes based on legitimate interest. However, as has been demonstrated above, the company did not retain any proof of the valid consent of the individuals, in breach of Article 7 of the GDPR. The company could not therefore restrict itself to halting the display of personalised advertising and effectively had to delete the data processed.
135. This conclusion is all the more necessary since it emerges from the investigations that the company processes a large volume of data which is established as having originated from cookies placed

before any expression of intention by the Internet user and even, in certain cases, when the user has expressly expressed his/her refusal.

136. It follows from the foregoing that in limiting itself to halting the display of personalised advertising and not deleting personal data in the event of exercise of users' right to erasure, for individuals for whom the company could not show meaningful consent, the company breached its obligations under Articles 7 and 17 of the GDPR.

G. On the violation of the obligation to provide for an agreement between joint controllers

137. Article 26 of the GDPR states that: "*1. [The joint controllers] shall in a transparent manner determine their respective liabilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them. 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects.*"
138. **The rapporteur** notes that on the date of the findings, the company had entered, with its joint controller partners (advertisers, publishers and online auction platforms), into a contract that contained a description of the processing that is the subject of joint responsibility and the role of each manager with regard to such processing.
139. It nevertheless emphasises that this agreement was not sufficient to lead to the conclusion that the company complies with Article 26 of the GDPR.
140. **The company** argues that, as drafted, the agreement with its partners did not harm data subjects, who have benefited from the full protection of the GDPR, since the general terms and conditions of use of its services specify that partners must provide a link to [REDACTED]'s privacy policy and allow data subjects to express their consent to targeted advertising.
141. Yet it explains that it has adopted a new agreement, which entered into force on 5 July 2022.
142. **The Restricted Committee** considers that the drafting of Article 35 of the GDPR shows that the deed of distribution of the obligations of joint controllers must cover all the obligations provided for by the GDPR in order to determine, for each of these obligations, which joint controllers will be responsible for them.
143. In this case, the Restricted Committee notes that on the date of the findings, the agreement entered into by the company with its partners did not specify some of the respective obligations of the data controllers with regard to the requirements contained in the GDPR, such as the exercise by the data subjects of their rights, the obligation to notify a data breach to the supervisory authority and to the data subjects or, where applicable, carrying out an impact assessment under Article 35 of the GDPR.
144. It points out that the obligation to enter into an agreement in the event of joint liability is a specific obligation imposed on joint controllers under Article 26 of the GDPR.

145. Although, in its version of 5 July 2022, the agreement entered into by the company with its partners now includes the information expected under this provision, the Restricted Committee notes that this late achievement of compliance does not alter the fact that a breach was committed in the past.
146. It follows from the above that the company breached its obligation under Article 26 of the GDPR.

III. On the issue of corrective measures and publicity

147. Article 20 of amended Act No. 78-17 of 6 January 1978 provides that: “*When the data controller or its processor does not comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this Act, the chair of the Commission nationale de l’informatique et des libertés (French Data Protection Authority) may [...] refer the matter to the Restricted Committee of the Commission with a view to imposing, after an adversarial proceeding, any one or more of the following measures: [...]*”
7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83”.
148. Article 83 of the GDPR, as referred to in Article 20, paragraph III of the French Data Protection Act, states: “*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive*”, before specifying the information to be taken into account when deciding whether to impose an administrative fine and when deciding on the value of such fine.

A. On the issue of an administrative fine and its amount

149. **The company** first argues that the CNIL infringed the principle of non-discrimination by bringing proceedings solely against it, despite having established that the websites of its partners did not comply with the regulations applicable to cookies.
150. It then argues that it should not be sanctioned for not ensuring that its partners obtain valid consent other than by contractual means, since such verifications should in fact be returned to the CNIL, which was thus engaging in a “privatisation” of its functions.
151. The company maintains that better consideration of the criteria laid down in Article 83(2) of the GDPR, in particular with regard to the absence of proof of damage, the non-intentional nature of the breaches, the measures taken to mitigate the damage, the cooperation it claims to have demonstrated with the supervisory authority, and the categories of personal data concerned, which are not particularly intrusive, would – should the Restricted Committee decide to impose a fine – justify a significant reduction of the 60 million euros amount proposed by the rapporteur.
152. It argues that the rapporteur’s proposed fine represents 50% of its profit and almost 3% of its worldwide turnover, which is close to the legal maximum under Article 83 of the GDPR. By comparison, it highlights the previous decisions handed down by the CNIL against Google (CNIL, FR, 31 December 2021, sanction deliberation no. SAN-2021-023) and Facebook (CNIL, FR, 31

December 2021, sanction deliberation no. SAN-2021-024) on cookies, the amount of which amounted to 0.07% and 0.06% of their overall turnover respectively.

153. **The Restricted Committee** recalls, as a preliminary point, that it is not the Restricted Committee's responsibility to assess the decision of the Chair of the CNIL to take legal action against the company alone.
154. The Restricted Committee notes that, in order to assess the appropriateness of imposing an administrative fine and establishing its value, it must take into account the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the infringement, the number of data subjects, the measures taken by the controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority, the categories of personal data concerned by the infringement and the financial benefits from the infringement.
155. Firstly, with regard to the imposition of an administrative fine, the Restricted Committee deems that it is in the first place appropriate to apply the criterion provided for in Article 83(2)(a) of the GDPR relating to the gravity of the infringement taking into account the nature, scope of the processing as well as the number of data subjects affected.
156. It points out, first of all, that it has been established that the company was unable to demonstrate that the data subjects had given their consent to the processing of personal data concerning them, and that the findings of the audit delegation revealed that the company used browsing data partially obtained from cookies placed before the Internet user had been able to exercise consent.
157. Next, with regard to the scope of the processing, the Restricted Committee stresses that the violation is all the more serious because the processing in question, which is aimed at displaying personalised advertisements, is carried out on a very large scale and is by nature widespread and intrusive.
158. It points out that in order for the displayed advertisements to be relevant, it is necessary for the company to collect large quantities of data relating to the browsing habits of Internet users in order to establish a precise picture of their consumption habits, preferences or concerns at the time.
159. This means that each visit to an advertiser's or publisher's site, each click on a product or each purchase made by an Internet user is recorded by the company and analysed for advertising purposes. As such, the company claims on its website that it collects 35 billion events per day from browsing and purchases worldwide. In addition, the company shares and receives data from its partners; for example, to enable it to better identify each Internet user or to establish a link between the various devices and browsers used by a single Internet user.
160. The Restricted Committee notes that, although when taken in isolation, each of the data items collected by the company has a low identifying value, when combined with each other, they could reveal with a significant degree of precision many aspects of people's private lives, including their gender, age and consumption habits, i.e. their tastes, thus giving the processing in question a widespread and intrusive nature.
161. Consequently, the result of the combination of this data considerably reinforces the widespread and intrusive nature of the processing in question and makes it even more necessary for it to be implemented in strict compliance with the rules in force, in particular those rules surrounding the choice of individuals as to the use of their data.

162. Similarly, the Restricted Committee points out that the transformation of raw browsing data into usable information constitutes the core activity of the company. The company must therefore be able to ensure that the personal data it processes complies with the regulations in force.
163. With regard to the number of individuals concerned by the processing in question, the Restricted Committee notes that the company publicly states that it has data relating to approximately 370 million user identifiers across the European Union, including approximately 50 million identifiers on French territory alone. Although a single individual may correspond to several identifiers, these figures reveal the substantial amount of data collected by the company.
164. As regards the violation related to informing individuals, the Restricted Committee emphasises that it has resulted in a loss of control by Internet users over their data insofar as the company has not provided them with complete and comprehensible information.
165. As regards the violations relating to the exercise of the rights of access, withdrawal of consent, and erasure, the Restricted Committee emphasises that these are structural in nature and are severe in that the measures introduced by the company lead not only to individuals' requests being incorrectly processed, but also to individuals legitimately believing that their request has been complied with.
166. It thus recalls that on the date of the findings, data subjects making access requests did not receive the data contained in two tables of the company's database.
167. The Restricted Committee also points out that the company's consideration of a request for erasure has no effect other than to stop the display of personalised advertisements, with the company also continuing to retain the data of the individual requesting the request and even using it for other purposes.
168. With regard to the breach of the obligation to provide for an agreement between joint controllers, the Restricted Committee considers that the fact of not having more precise supervision of the processing carried out jointly with other stakeholders has deprived the data subjects of the full protection of their personal data afforded by the GDPR.
169. Secondly, the Restricted Committee considers that it is appropriate to apply the criterion set out in Article 83(2)(k) of the GDPR related to the financial benefits gained from the infringement.
170. It points out that the company's business model is based exclusively on its ability to display the most relevant advertising to Internet users to promote the products of its advertising customers, and therefore on its ability to collect and process a huge amount of personal data.
171. However, it emerges from this procedure that this collection and the processing in question are in breach of the requirements of the GDPR and the rights of data subjects, since the company is accused of not being able to demonstrate that these data subjects have given their consent to the processing of their data and that it has been established, in certain cases, that the company processed data for which the data subjects had not consented or had not given valid consent.
172. This means that the personal data collected and processed without valid consent of the individuals have enabled the company to unduly increase the number of individuals concerned by its processing, and therefore its financial income.

173. The Restricted Committee adds that the company also gained a financial advantage because it did not erase data by continuing to use data that had not been erased for the purpose of improving its technologies, which contributes to its competitiveness in the targeted advertising market.
174. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the breaches of Articles 7, 12, 13, 15, 17 and 26 of the GDPR.
175. Secondly, with regard to the determination of the amount of the fine, the Restricted Committee points out that pursuant to the provisions of Article 20(III) of the French Data Protection Act and Article 83 of the GDPR, the company is incurring, in respect of the established breaches mentioned above, a financial penalty of a maximum amount of 20 million euros or 4% of its total worldwide turnover of the previous financial year, [REDACTED], whichever figure is the higher.
176. Therefore, in view of the company's liability, its financial capacities and the relevant criteria of Article 83(2) of the Regulation, referred to above, the Restricted Committee considers that a fine of forty million euros appears to be justified.
177. It notes that although the amount of the proposed penalty actually constitutes [REDACTED] of the company's worldwide turnover, it nevertheless remains below the legal ceiling of 4% provided for in Article 83(5) of the GDPR and Article 20(III, (7)) of the French Data Protection Act.
178. Furthermore, the Restricted Committee points out that the value of the fine may be higher than the profit generated by the data controller, insofar as this would be necessary to ensure the deterrent nature of the penalty (in this respect, see: EC, 1 March 2021, *Futura Internationale company*, no. 437808, pt. 6).

B. On publication of the decision

179. The company asks the Restricted Committee to not make its decision public.
180. However, the Restricted Committee considers that publication of this decision is justified in the light of the severity of the breach in question, the scope of the processing and the number of data subjects concerned.
181. It also notes that this measure will enable the data subjects to be informed of the existence of the processing carried out by the company and of the fact that it was able to process their data without their knowledge, or even despite their lack of consent. By being informed in this way, they will, where applicable, be able to assert their data protection rights vis-à-vis the company.
182. Finally, it considers that this measure is proportionate since the decision will no longer identify the company by name upon expiry of a two-year period following its publication.

FOR THESE REASONS

The CNIL's Restricted Committee after having deliberated, decided to:

- **impose an administrative fine against [REDACTED] SA in the amount of forty million euros (€40,000,000) with regard to the established breaches of Articles 7, 12, 13, 15, 17 and 26 of the GDPR;**
- **make its deliberation public, on CNIL's website and on the Légifrance website,** the deliberation no longer identifying the company by name upon expiry of a period of two years following its publication.

The Chair

Alexandre Linden

This decision may be appealed before the Conseil d'Etat within two months of its notification.

Summary Final Decision Art 60 Complaint

EDPBI:FR:OSS:D:2023: 809

Violation identified ; Administrative fine

Background information

Date of final decision:	15 June 2023
Date of broadcast:	22 June 2023
LSA:	FR
CSAs:	All SAs
Legal Reference(s):	Article 7 (Conditions for consent) , Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 13 (Information to be provided where personal data are collected from the data subject), Article 15 (Right to access by the data subject), Article 17 (Right to erasure ('right to be forgotten')) Article 26 (Joint controllers).
Decision:	Administrative fine, Violation identified.
Key words:	Transparency, Right of access, Data subject rights, Exercise of data subject rights, Consent, Definition of controller, Right to erasure, Advertising, Cookies.

Summary of the Decision

Origin of the case

The controller is a company registered in France ("the company"). It specialises in the display of targeted advertising online, including in advertising retargeting. The LSA received two complaints in 2018, following which it carried out online and onsite audits and sent requests for information to the company. The company collects browsing data from Internet users through cookies that are stored on their terminals when they visit one of the controller's partners' websites. When an Internet user visits a partner's website, the company stores a cookie on the device his or her browser is running on. In practice, a unique identifier is assigned to the data subject (i.e. an "ID"), which will enable the company to recognise him/her during subsequent visits to the partner's other sites. The company acts as an intermediary between advertisers and website publishers and engages in "real-time bidding" (RTB) for displaying an ad on the publisher's advertising space. If the company wins the bid, an advertiser's advertising banner is displayed in the ad space available on the publisher's website.

Findings

According to the LSA, although the company does not directly hold the identity of the data subjects to which the devices on which cookies are dropped are linked, it is able to re-identify individuals by reasonable means. The company acts as a **controller, jointly with its partners** (advertisers, publishers, online auctions platforms).

The LSA analysed the **legal basis** relied upon for the retargeting processing activity. While the company claimed that it relied on consent, it was unable to provide any proof of user consent. The LSA points out that in the case of joint controllership, Article 26 GDPR requires that joint controllers ensure - through an agreement - that they mutually comply with the GDPR and in particular that they work together to determine the best way to respond to the rights of data subjects, depending on the nature of the processing and their respective responsibility for such processing. It considers that the mere fact that the collection of user consent for the given processing constitutes the partners' contractual obligation does not exempt the company from its obligation to be able to demonstrate that the data subject has given his/her consent under Article 7 GDPR. This dual-liability regime ensures that at all stages of the processing, each joint data controller complies with the provisions incumbent upon it: for partners, those relating to the storage and reading of the company's cookie on the user's device and for the company, those provisions relating to subsequent processing carried out based on the data collected by this cookie. In addition, the LSA's online audits showed that some of the partners' websites did not obtain valid user consent.

The LSA notes that the company became compliant with Article 7(1) GDPR progressively over the course of the investigation, including by implementing an audit program to scan the compliance of its partners since 2020, by terminating a contract concluded with a non-compliant partner and by requiring contractually that its partners provide a **proof of user consent**.

In addition, the LSA found that the company was in breach of its **transparency obligations** under Articles 12 and 13 GDPR. More specifically, the LSA concluded that Article 13 GDPR applies to the company, given that when users browse the website of a partner of the company, the cookie requests are sent directly to the company's servers, without transiting via another data controller. The LSA

considered that before updating the privacy notice over the course of the proceedings, the company's privacy notice did not make it clear what the applicable legal basis was under Article 6 GDPR and included a vague and contradictory description of the processing purposes. Lastly, the privacy notice did not make it clear that personal data was processed for a separate purpose, namely to improve the company's advertising services through machine learning.

Furthermore, the LSA concluded that the company did not comply with the **exercise of the right of access under Articles 12 and 15 GDPR**. The company did not provide data subjects with all the personal data relating to them and did not allow them to fully understand the information provided.

The LSA also considered that the company did not comply with the **exercise of the right to erasure under Articles 7 and 17 GDPR**. In fact, when it responds to a request for erasure, the company does no more than stop the display of personalised advertisements on the device of the individual making the request, without effectively deleting the data relating to that individual.

With respect to joint controllership, the LSA considered that the company breached its obligations under Article 26 GDPR. On the date of the findings, the agreement entered into by the company with its partners did not specify some of the respective obligations of the data controllers with regard to the requirements contained in the GDPR, such as the exercise by the data subjects of their rights, the obligation to notify a data breach to the supervisory authority and to the data subjects or, where applicable, carrying out a data protection impact assessment under Article 35 GDPR.

Decision

The LSA imposed on the company an administrative fine of **40 million euros for the infringement of Articles 7, 12, 13, 15, 17 and 26 GDPR**. 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. To set the amount of the administrative fine, the LSA took into account the severe character of the infringements found. This stems from the fact that the processing activity is large-scale and intrusive by nature given the large volume of collected browsing data and the very high number of affected data subjects. . The LSA also highlighted the consequences for data subjects, including a loss of control of users over their personal data online and an undermined protection of their personal data. The LSA also noted that the company's core activity consists in enriching the "raw" data. Lastly, as the company's business model relies on displaying targeted advertising, the failure to obtain valid user consent has enabled the company to process more personal data, thereby making more profit.

Deliberation of the Restricted Committee No. SAN-2023-003 of 16 March 2023
concerning [REDACTED]

The *Commission nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr Alexandre Linden, Chair, Mr Philippe-Pierre Cabourdin, Vice Chair, Ms Anne Debet, Mr Bertrand du Marais, and Mr Alain Dru, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data, in particular Articles 56 and 60;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 *et seq.*;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Agency);

Having regard to Decision No. 2020-081C of 12 May 2020 of the Chair of the *Commission Nationale de l'Informatique et des Libertés* (CNIL) to instruct the general secretary to carry out or have a third party carry out an assignment to verify all of the processing related to the “[REDACTED]” application for smartphones;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 12 April 2021;

Having regard to the report of Ms. Valérie Peugeot, commissioner rapporteur, notified to [REDACTED] on 17 March 2022;

Having regard to the written observations made by [REDACTED] on 02 May 2022;

Having regard to the response of the rapporteur notified to the company on 16 June 2022;

Having regard to the written observations of [REDACTED] received on 29 July 2022 and the oral observations made at the Restricted Committee meeting;

Having regard to the other exhibits;

The following were present at the restricted committee session on 29 September 2022:

- Valérie Peugeot, commissioner, her report having been heard;

In the capacity of representatives of [REDACTED]:

- [REDACTED];
- [REDACTED].

[REDACTED] having spoken last;

The restricted committee has adopted the following decision:

I. Facts and proceedings

1. [REDACTED] (hereinafter “the company”) is a French simplified joint stock company [REDACTED] [REDACTED], located at [REDACTED] and created in 2014. The company estimates that there are [REDACTED] in its workforce in France. In 2019 it generated a turnover of [REDACTED] for a net loss of [REDACTED]. In a letter dated 21 April 2021, the company estimated its turnover for the financial year ended 31 December 2020 at [REDACTED] and a loss of [REDACTED].
2. Since 2016, the company has offered a self-service electric scooter rental service that can be accessed from the [REDACTED] mobile application. It is a “free-floating” vehicle sharing offer, i.e. there are no stations. The scooters are therefore not parked in specific spaces and can be left after use in the rental area identified in the application. The scooters are equipped with an on-board localisation device that allows [REDACTED] and users, via their mobile application, to know the location of the scooters. Renting an electric scooter from the company requires an account to be created using the mobile application. This is a non-binding service which is charged by the minute.
3. In France, this service is available in the Paris region and in Nice. Furthermore, the company has also expanded its service in certain cities in Italy and Spain through two wholly-owned subsidiaries, [REDACTED] and [REDACTED]. To date, the company has approximately [REDACTED] users in France and abroad.
4. An online check was carried out on the website “[REDACTED]” and the mobile application “[REDACTED]”, on 13 May 2020. Record No. 2020-081/1 drawn up at the end of this audit was notified to [REDACTED] on 19 May 2020. The CNIL delegation particularly focused on verifying the data collected and the purposes of its collection. The purpose of this check was also to verify the supervision of subcontracting and data security.
5. Three requests for additional information were then sent to the company by recorded delivery letter dated 26 June 2020 and by email dated 27 August and 10 December 2020. The company responded to these requests by letters dated 16 July, 11 September and 15 December 2020.
6. In accordance with Article 56 of the GDPR, on 27 February 2020, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by [REDACTED], namely the management of user accounts set up by [REDACTED] derived from the fact that [REDACTED]'s principal establishment is located in France. After exchanges between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, Spain and Italy are declared to be covered by this processing.
7. In order to examine these items, the CNIL Chair appointed Valérie Peugeot as rapporteur on 12 April 2021, pursuant to Article 22 of the amended French Data Protection Act of 6 January 1978.

8. On 17 February 2022, the rapporteur sent the company an additional request relating to the anonymisation of personal data made by hashing the data and the application of a salt. The company responded in a letter dated 23 February 2022.
9. The rapporteur notified [REDACTED] on 17 March 2022 of a report detailing breaches of the provisions of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 (hereinafter “the Regulation” or the “GDPR”) and amended Act No. 78-17 of 6 January 1978 on data processing, files and freedoms (hereinafter “the French Data Protection Act” or “amended Act of 6 January 1978”) which it considered established in this case. This report also proposed that the restricted committee of the CNIL impose an administrative fine against the Company and that this decision be made public but that the Company not be identifiable by name upon expiry of a period of two years following its publication.
10. On 02 May 2022, the company submitted observations in response to the Rapporteur’s sanction report.
11. By letter dated 16 June 2022, the rapporteur's response was sent to the company.
12. On 29 July 2022, the company submitted further observations in response to those of the Rapporteur.
13. In a letter dated 22 August 2022, the rapporteur informed the company of the completion of the investigation.
14. On 23 August 2022, the Chairman of the restricted committee notified [REDACTED] of a convocation to its meeting on 29 September 2022.

II. Reasons for the decision

15. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 15 February 2023.
16. As of 15 March 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

A. On the breach of the obligation to ensure the appropriateness, relevance and non-excessive nature of the personal data processed by the company in accordance with Article 5(1)(C) of the GDPR

17. Article 5(1)(c) GDPR provides that personal data shall be “*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimisation”)*”. When the data is collected on the basis of the legitimate interest, this collection must also not disproportionately cause a breach of privacy rights regarding the objectives pursued by the company.

18. **The rapporteur** notes that, within the framework of the investigation, the CNIL's inspection delegation was informed that the scooters are equipped with electronic boxes including a SIM card and a GPS geolocation system, embedded on the scooters. She added that these units collect location data from scooters every 30 seconds when the [REDACTED] is active and its dashboard is on, whether it is moving or ready to be driven. When the [REDACTED] is not active, the unit collects location data every 15 minutes.
19. This data is then stored in a “scooter database” which contains the following data: the location via GPS and “*a reservation number [...] that is collected if the [REDACTED] is reserved, during the rental period*”. They are stored in an active database for 12 months, then 12 months in intermediate archiving before being anonymised.
20. The company also stated that the collection of scooter location data, namely the location of the scooter at the reservation departure and arrival points and the location throughout the journey, has the following purposes: handling traffic offences, handling customer complaints, user support (in order to call the emergency services if a user falls off), claims and handling thefts.
21. To end a rental, the user must carry out certain manipulations such as: make sure to be in an authorised area to park the scooters ([REDACTED] zone), switch off the scooter, press the “END” button located on the scooter or click on “END MY RENTAL” in the mobile application and check that the green diode “FREE” is lit.
22. The rapporteur considers that none of the purposes put forward by the company justify the almost permanent geolocation data collection during the rental of a scooter.
23. **The relevance of collecting this data for each of these purposes should be examined.** First of all, the Restricted Committee points out that, when a vehicle is being rented, geolocation data from the vehicle is associated with an individual and constitutes personal data. However, when the scooter is not rented, geolocation data related to the vehicle alone is not personal data.
24. The restricted committee notes that the company uses three distinct databases:
- a “scooter database” which contains the data transmitted by sensors fixed to the scooter (scooter location via a GPS, battery status, saddle sensor);
 - a “reservation database” which contains the start and end dates and times of each rental as well as the scooter's condition at the start and end of its rental;
 - a “customer database” which includes data for handling invoicing. This database does not contain scooter data.
25. The restricted committee notes that, while scooters' position data are decorrelated from any information relating to users in the “scooter database” and are kept in a database separate from that storing user data, i.e. the “customer database”, which constitutes a choice of privacy-friendly computer architecture (privacy by design), the fact remains that this data may be combined with the data present in the other databases, in particular through the reservation number present in each of the databases, giving extensive and simultaneous access to the databases.

26. The restricted committee therefore considers that the geolocation data collected by [REDACTED] while the scooter is being rented is personal data when it is possible to combine the different databases, even if such a combination is only one-off, the scooter position data relating to an identified or identifiable natural person.
27. The rapporteur notes that while geolocation data is not sensitive data within the meaning of Article 9 of the GDPR, it is nevertheless considered by the Article 29 Working Party (called the “G29” which became the European Data Protection Board (EDPB) in its guidelines of 04 October 2017, as being “highly personal data”. The EDPB believes that such data is considered to be sensitive data, as the term is commonly understood, insofar as it affects the enjoyment of a fundamental right: collecting position data threatens freedom of movement.
28. By way of clarification, the Restricted Committee also points out that the EDPB considered, in its guidelines 01/2020 on the processing of personal data in the context of connected vehicles and applications related to mobility (Guidelines 01/2020) that “*When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data is particularly revealing of the life habits of data subjects. The journeys undertaken are very characteristic in that they enable one to infer the place of work and of residence, as well as a driver’s centres of interest (leisure), and may possibly reveal sensitive information such as religion through places of worship, or sexual orientation through places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controllers should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing*”. These guidelines also emphasise that the location data collection is subject to compliance with the principle on which location can be activated “*activating location only when the user launches a function that requires the vehicle’s location to be known, and not by default and continuously when the vehicle is started*”.
29. Although the company disputes the applicability of the guidelines to the present case on the grounds that they only concern cars, the restricted committee considers that the guidelines are relevant for geolocation data in general.
30. In this context, the Restricted Committee points out that the assessment of compliance with the principle of data minimisation is based on the limited nature of the data processed regarding the purpose for which it is collected. Its assessment implies performing an analysis of the proportionality of the personal data collection regarding the purposes for which it is intended.
31. In view of the foregoing, the restricted committee considers that only the need for the collection and retention of position data collected every 30 seconds should be analysed when the collection of position data at the beginning and end of the lease is relevant to the purposes pursued.
32. **Firstly, regarding the management of claims related to additional charges, the rapporteur** considers that the collection of geolocation data every thirty seconds for the entire duration of the rental is not necessary. The rapporteur specifies that the management of overcharging should be managed by the user's contact when he/she encounters a difficulty in terminating his/her rental or, at the very least, by less intrusive means than almost permanent geolocation of the vehicle throughout the lease.

33. In its defence, **the company** argues that the collection of the position data of the scooters every 30 seconds would be necessary, as part of a service invoiced by the minute for situations that have led to overcharging and claims from users when they have failed to properly terminate their rental, in particular when:

- the user loses communication with a scooter for technical or human reasons;
- the user makes a complaint related to unauthorised parking areas;
- the user does not stop the scooter correctly to end the rental;
- the scooter is moved by a third party.

34. The collection of position data every 30 seconds would make it possible to go back in 30 seconds steps to identify the number of seconds during which the scooter was stopped. It adds that users very often realize later that a rental was not properly completed and do not contact the company when the rental is terminated. The triggering of geolocation at the time of contact by the user would not therefore suffice because it would not be possible to calculate the additional charge minutes between the time the user wanted to end the rental and could not do so, and the time when the company was able to solve the problem and put an end to the rental.

35. **The Restricted Committee** notes the arguments put forward by the company about managing complaints related to additional charges. However, it notes that, for this purpose, the collection and retention of geolocation data for scooters every 30 seconds is not necessary.

36. Indeed, in three of the situations mentioned by the company (loss of communication with the scooter, difficulty related to unauthorised areas, scooter displaced by a third party), the restricted committee considers that the user can contact [REDACTED] to resolve the difficulties and complete the rental. Geolocation could therefore be triggered from this generating event.

37. Regarding cases where the user does not stop the scooter correctly to end the rental, the restricted committee points out that the geolocation of the scooter every 30 seconds does not make it possible to determine when the user really wanted to end the rental. Indeed, the static position of the scooter alone does not demonstrate the user's desire not to continue the rental.

38. In addition, the restricted committee states that it would be possible to put in place alternative and less intrusive mechanisms allowing the company to ensure that the user has terminated the rental or, on the contrary, warn it when this is not the case, for example by sending an SMS message or confirmation by an alert via the application that the rental has ended.

39. Although for the month of June 2022 the company claims to have received approximately 11,500 calls for 386,766 journeys relating to additional charge problems, it does not indicate what proportion of the calls related to this specific situation. The restricted committee considers, in the absence of precise statistics, that these cases cannot justify the almost permanent geolocation of all scooters.

40. In general, the rapporteur notes that Article 7.4.6 of [REDACTED]'s General Terms and Conditions of Use provides that "it is the Users' responsibility to check that their Rental has ended correctly. [REDACTED] shall not be held liable for prolonged invoicing in the event of incorrect return of the Scooter". It is therefore up to the user to ensure that he/she has properly terminated the rental.
41. **Secondly, regarding the management of fines, the rapporteur** considers that the geolocation data of the scooters throughout the journey are not necessary to identify the user responsible for an infringement when a check of the time of the infringement and the person who leased it during this period is sufficient to do so.
42. In its defence, **the Company** asserts that collecting scooter positioning data every 30 seconds is necessary to obtain information about the circumstances and context in which the infringement was committed. The objective is to verify whether the infringement identified by the ANTAI ("National Agency for Automated Processing of Offences") has been committed: confirm or disprove the presence of the scooter at the place identified by the notice of violation and verify whether the offence could have occurred in this place. It also considers that the collection of scooters' position data is necessary in order to be able to identify or prove the identity of the driver to the ANTAI, the police or the insurance companies.
43. **The restricted committee** considers, on the one hand, that it is not necessary for the company to collect and retain the position of the scooters every 30 seconds to identify and prove the identity of a driver to the ANTAI, the policy or the insurance companies. In fact, collecting the number and date of the infringement notice, the date and time of the start and end of the lease and the date and time of the infringement is sufficient to meet this purpose. This data, cross-referenced with the registration plate number of the scooter, makes it possible to identify the person who leased said scooter. Moreover, collecting the position data of the scooters does not make it possible to establish as such the identity of the person responsible for the offence since it is not possible to determine whether the scooter was moved by the person who leased it or whether it was moved by a third party to an illegal parking area since scooters can be freely moved with or without the motor in operation.
44. Moreover, the restricted committee considers that collecting scooter positioning data every 30 seconds is excessive in that this data is collected for all the vehicles leased by the company although doing so only meets an incidental purpose when a given user needs the data to dispute a traffic infringement.
45. **Thirdly, regarding the management of vehicle theft, the rapporteur** stresses that, in order to be considered proportionate, the processing of geolocation data must be made necessary for this purpose by a triggering event, such as a reported theft or suspected theft. The geolocation data of the scooters cannot therefore be considered strictly necessary for the pursuit of the purpose related to the risk of theft before any triggering event.
46. In its defence, **the company** asserts that the collection of scooter data in the event of theft does not mean that this data is matched with the identity of the users. The company adds that it only needs scooter location data to be able to locate scooters in order to find and recover them in the event of theft.

47. The company states that it cannot rely solely on the indications of the last position provided by the user at the time of the declaration of theft, which are not necessarily reliable and that certain technical difficulties (flat battery, technical problem or when the scooter is in a car park or an area in which geolocation cannot be triggered) may prevent it from triggering remote geolocation. It also states that the collection of scooters position data every 30 seconds significantly reduces the search area in the event of theft and that the geolocation system, which is integrated into the scooter, cannot be deactivated by a person seeking to steal the scooter.
48. **The restricted committee** points out above all that, even if the company does not match the position data of the scooters and the user's data to find stolen vehicles, the possibility of this matching between the different databases justifies the position data of the scooters being considered personal data and subject to the requirements of the GDPR.
49. The rapporteur also points out that before any triggering event, vehicle geolocation data cannot, as a rule, be regarded as strictly necessary for pursuing this purpose and its continuous collection or collection at very close intervals must be considered excessive.
50. By way of clarification, the Restricted Committee finds that the Guidelines 01/2020 state that location data can only be passed on after a reported theft and cannot be constantly collected for the rest of the time. In this respect, the EDPB also recommends that the data controller should clearly inform the data subject that the vehicle is not permanently tracked and that geolocation data can only be collected and transmitted after a reported theft.
51. In addition, the Restricted Committee stresses that assessing if processing is limited to what is necessary, within the meaning of Article 5(1)(c) GDPR, is informed by the provisions of recital 39 GDPR, according to which, "*Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means*". The existence of less intrusive means of achieving the same purposes must thus be taken into account, whether processing data by alternative means or processing less data, or processing it less frequently.
52. Above all, the restricted committee specifies that if the scooter is stolen outside a rental period, the scooter's position data is not linked to a reservation and therefore does not identify an individual. This is therefore not personal data and such a situation is therefore outside the scope of this procedure.
53. The restricted committee then goes on to consider that no theft scenario justifies collecting position data every 30 seconds. On the one hand, cases, for which the company has not established the frequency, where the scooter is stolen during use, i.e. when the user is him/herself on the functioning scooter, does not justify the quasi-permanent collection of scooter position data. On the other hand, scooters can be stolen when users takes a break during the rental. In this situation the user may contact [REDACTED] immediately upon confirmation of the theft at the end of the break, which will inform the company of the last position of the scooter.

54. Questioned on the number of vehicles found thanks to the latest known position of the scooter, the company was unable to provide statistics showing the effectiveness of geolocation every 30 seconds.
55. Thus, the Restricted Committee points out that, in view of the above considerations, cases where, on the one hand, geolocation is the only way of knowing the last known position of the vehicle and where, on the other hand, the last known position is actually close to the location of the vehicle, appear to be limited. In such situations, the Restricted Committee does not call into question the need to know the last known position of the vehicle using the latest geolocation data. But this assumption is not sufficient to justify the collection of all geolocation data for all users' journeys.
56. In the light of all these considerations, the Restricted Committee considers that, in many use cases, collection of geolocation data every 30 metres during the scooter rental is not necessary for managing theft of vehicles. The fact of systematically carrying out this collection for situations where it could actually be useful on the basis of the legitimate interests of the company, appears to be a disproportionate breach of privacy rights. Indeed, as pointed out above, the company's collection and retention of all vehicle user journeys lead it to handling and retaining highly sensitive data (cf. CNIL, FR, 7 July 2022, Sanction, [REDACTED], No. SAN-2022-015, published).
57. **Fourthly, regarding the management of accidents, the rapporteur** argues that the collection of geolocation data for this purpose can only take place from a triggering event, particularly technical notification when the scooter is at an excessively steep angle or there is a request for assistance by the customer, making such collection necessary.
58. In its defence, the company maintains that it is necessary to collect scooter location data every 30 seconds and to cross-reference it with the user data, to be able to contact the user when the detector has sent a technical warning relating to an accident and to assist the user with declaration and reporting formalities. The company adds that accidents do not necessarily trigger a technical notification, particularly when the scooter is not at a sufficiently steep angle. The company states that it is regularly contacted by insurance companies after a claim to obtain additional information such as the precise location of a scooter at the time of an accident.
59. **The Restricted Committee** first points out that it is entirely legitimate for the company to wish to assist users who are victims of traffic accidents during the rental of a vehicle. However, in order to provide such assistance to users, the company must be aware that an incident or accident has occurred.
60. The Restricted Committee considers that, as soon as the company becomes aware of the occurrence of an accident concerning a rented vehicle, it may geolocate this vehicle in order to assist the user if necessary.
61. The restricted committee considers that, in the vast majority of cases, a triggering event allows the company to be aware of an accident, whether it is the technical notification of the scooter being at an excessively steep angle or a call from the user.

62. On the other hand, the Restricted Committee considers that geolocation every 30 meters of all scooters throughout the rental term, prior to receiving any information relating to an accident, is not necessary to provide assistance to a user. The near permanent geolocation data collection is therefore neither appropriate nor relevant to this purpose.
63. **It follows from all of the above that the Restricted Committee considers that none of the purposes advanced by the company justify collecting geolocation data every 30 metres during the rental of a vehicle. Such a practice is indeed very intrusive to the privacy of users insofar as it can reveal their movements, the places they visit, and all the stops made during a journey, which amounts to calling into question their freedom to move freely.** The Restricted Committee notes in this respect that it is clear from the foregoing that the company could offer an identical service without near constant geolocation data collection.
64. The Restricted Committee therefore considers that these facts constitute a breach of Article 5(1)(c) of the GDPR.

B. On the failure to define and respect a personal data storage period, which is proportionate to the purposes of the processing, in accordance with Article 5 (1)(e) of the GDPR (storage limitation)

65. Article 5(1)(e) of the Regulation requires that personal data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')*".
66. **The rapporteur** pointed out, in her report, that it appears from the exchanges with the company that the position data are kept in the scooter database without any time limitation, while the company also specifies that these data are anonymized after twenty-four months. The rapporteur considered that keeping user's geolocation data for an unlimited period of time or for twenty-four months in the active database exceeds the period of time necessary for the purposes for which the data concerning management of customer complaints and management of fines, damages and thefts are processed.
67. **In its defense, the company** explained that, contrary to what was stated in the report, it doesn't keep personal data "*without time limitation*" and not during twenty-four months in active database. It specified that the scooters' position data are kept for twelve months in active database, and that after twelve months, the scooters' position data are no more kept in active database but are archived in an intermediate database. After this storage of twelve months in intermediate filing, the data are anonymized.

68. **During the session**, given the information communicated by the company as part of the investigation, the rapporteur considered that the period and conditions of retention comply to the GDPR, in view of the purposes mentioned.

69. The restricted committee considers that the breach of Article 5(1)(e) of the GDPR is not constituted.

C. On the failure to provide a formal legal framework for the processing operations carried out by a sub-contractor in application in article 28, paragraph 3 of the RGPD

70. Article 28 of the GDPR requires that the processing carried out by a subcontractor for a data controller be governed by a contract which sets out the aim and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects concerned and the obligations and rights of the data controller. This contract also provides for the conditions under which the subcontractor undertakes to perform the processing operations on behalf of the data controller.

71. **The rapporteur** found that [REDACTED] uses fifteen subcontractors with access to or hosting of personal data. Of these fifteen contracts, she considers that the contracts with [REDACTED], [REDACTED], [REDACTED], [REDACTED] and [REDACTED] do not contain all the information provided for in the GDPR. The contract with [REDACTED] only generally provides for the security obligations incumbent on the subcontractor and it does not mention the obligation on the subcontractor to make all information available to the data controller to demonstrate compliance with the obligations provided for, enable audits to be carried out and contribute to these audits. The contract with [REDACTED] does not stipulate a procedure for the deletion or return of the subcontractor's personal data to the data controller upon expiry of the contract. The contract with [REDACTED], which is very incomplete, does not state the purpose of the processing or its duration. Finally, the contract with [REDACTED] does not cover the category of data subjects concerned by the processing.

72. In its defence, **the company** states that the contracts with [REDACTED] and [REDACTED] have been amended following inspections by the CNIL in order to comply with the GDPR. Regarding the contract with [REDACTED], the company considers that the subcontractor undertakes to implement the measures required by Article 32 of the GDPR and that the contract provides for the conditions under which the subcontractor makes the necessary information available to [REDACTED]. Regarding the contract with [REDACTED], the company states that the data is processed in accordance with the subcontractor's data retention policy according to which any data is deleted or erased after the end of the retention period, which is 14 months before anonymisation.

73. **The restricted committee** points out, as a preliminary point, that in its guidelines 07/2020 of 7 July 2021 on the concepts of controller and subcontractor in the GDPR, the EDPB states that "*while the elements referred to in Article 28 of the Regulation constitute the essential content of the contract, the contract should allow the controller and the subcontractor to further*

clarify how these essential elements will be implemented by using detailed instructions. Therefore the processing agreement should not merely reproduce the provisions of the GDPR; it should include more specific and concrete information on how the conditions will be met and on the level of security required for the processing of personal data that is the subject of this agreement” (paragraph 112). Therefore the information referred to in Article 28(3) must not only be included in the subcontracting contract, but must also be sufficiently precise and detailed to ensure that the personal data is processed in a compliant manner.

74. Regarding the contract concluded with [REDACTED], the “accountability” clause effectively provides that the subcontractor must answer the data controller's questions and provide any document requested. However, it is not clearly stated that the subcontractor must, upon request, make all information available to enable audits to be carried out and take part in these audits.
75. The rapporteur also considers that the “*security clause, which requires that the subcontractor implement technical and organisational measures to ensure a level of security suited to the risk, should be more specific*”. Indeed, by way of illustration, in its guidelines 07/2020, the EDPB states that “*the agreement should avoid merely repeating these assistance obligations and should contain details on how the subcontractor is invited to assist the controller in fulfilling the obligations listed. For example, standard procedures and forms may be attached as appendices to the agreement to enable the subcontractor to provide the controller with all necessary information [...] the subcontractor is first required to assist the controller in complying with the obligation to adopt appropriate technical and organisational measures to ensure the security of the processing. Although this may, to some extent, encroach on the requirement that the subcontractor itself adopt appropriate security measures where the subcontractor's processing operations fall within the scope of the GDPR, these two obligations remain distinct, one referring to measures specific to the subcontractor and the other to those of the controller*”. Here, only the security objectives to be achieved are described, without specifying how to achieve it, such as a description of the processes or mechanisms developed in appendices to the contract. In the absence of clarification on the means to fulfil the obligation to implement technical and organisational measures to ensure a level of security appropriate to the risk, the restricted committee considers that the contract does not meet the requirements of the GDPR.
76. Regarding the contract concluded with [REDACTED], the rapporteur considers that while the contract provides for a personal data retention policy, no mention is made of the fate of the data in the event of termination of the contract between the two companies. Indeed, the data retention period policy and the fate of the data at the end of the contract are the subject of two different references under Article 28(3) of the GDPR and must therefore be specifically and separately referred to in the contract. Article 28(3) (g) provides that the contract must indicate that the subcontractor “*at the choice of controller, delete all personal data or return it to the controller at the end of the provision of services relating to the processing, and destroy existing copies*”. Therefore this phrase must therefore be specifically and separately referred to in the contract.
77. Regarding the contracts with [REDACTED] and [REDACTED], the restricted committee takes note of the fact that the company has ensured that the contracts comply with the requirements of the GDPR. However, at the date of the audits, the said contracts did not meet these requirements. Indeed, the contract with [REDACTED], which is very incomplete,

did not concern in particular the purpose of the processing, the duration of the processing or the type of personal data processed. As concerns the contract entered into with [REDACTED], it did not specify the category of persons covered by the processing.

78. Therefore regarding all of these facts, the Restricted Committee considers that the breach of Article 28 (3) of the GDPR is established.

D. Regarding the breach of the obligation to notify users and obtain their consent before recording and reading data from their electronic communications devices, in violation of Article 82 of the French Data Protection Act.

79. Article 82 of the French Data Protection Act provides that “*any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he/she has been previously informed by the data controller or its representative, of: 1) the purpose of any action aimed at electronically accessing information already stored in his or her electronic communications terminal equipment, or recording information on this equipment; 2° The means available to him or her to object to it. Such access or recording may only take place provided that, after receiving such information, the subscriber or user has expressed his or her consent which may result from the appropriate parameters of his/her connection device or any other device under his or her control. These provisions shall not apply if access to the information stored in the user's terminal equipment or the recording of information on the user's terminal equipment: 1° Is for the exclusive purpose of allowing or facilitating electronic communication; 2° Or is strictly necessary for the provision of an online communication service at the express request of the user*”.

80. **The rapporteur** considers that [REDACTED], as the publisher of the website ‘[REDACTED]’ and the mobile application [REDACTED], has a responsibility for compliance with the obligations of Article 82 of the French Data Protection Act for the operations of reading and/or writing data performed in users' terminals via the reCaptcha mechanism provided by Google when creating an account on the mobile application as well as when logging in and using the forgotten password procedure on the website. The rapporteur notes that [REDACTED] does not provide any information, in particular through a consent window, regarding the collection of information stored on user equipment or the means to refuse such collection. Furthermore, the user's consent regarding accessing information stored on his/her equipment or recording information on his/her equipment is not collected at any time.

81. In its defence, [REDACTED] states that it uses the reCaptcha mechanism for the sole purpose of making the user authentication mechanism secure. It states that setting up such a mechanism complies with CNIL deliberation No. 2017-012 of 19 January 2017, which does not specify that it is mandatory to obtain the consent of users. It adds that the use of reCaptcha must be covered by the second exemption provided for in Article 82 of the French Data Protection Act in that the service is requested by the user - namely registration or connection to the [REDACTED] service - and that the actions to read and write data on the terminals are necessary to ensure the security of the service. Lastly, the company states that as it is not required to obtain the consent of its users for its own use of the reCaptcha mechanism, it cannot be required to

obtain the consent of its users on behalf of Google. It states that the Google reCaptcha mechanism, which is directly integrated into the website, provides a link that refers to Google's privacy policy, implying that Google considers itself a data controller and informs users itself. Furthermore, [REDACTED] cannot itself modify the presentation or configuration of the mechanism and therefore does not have the ability to integrate a check box or another information link. The company states that deliberation No. 2020-092 of 17 September 2020 is later than the control procedure and cannot be applied to judge whether user consent has been obtained, such judgement being carried out on the regime prior to the said deliberation. However, it concludes that it will no longer use this mechanism as of October 2022.

82. **The restricted committee** notes, **firstly**, that the Council of State ruled (CE, 6 June 2018, *Editions Croque Futur*, No. 412589, Rec.), that under the obligations incumbent on the publisher of a site that places "third-party cookies", include that of checking with its partners, on the one hand, that they do not issue trackers through the site that do not comply with the regulations applicable in France, and on the other hand, to take any useful steps with them to put an end to any breaches. In particular the Council of State judged that "*website publishers who authorise the placing and use of said "cookies" by third parties when their website is visited must also be considered as data controllers, even though they are not subject to all the obligations imposed on third parties who have issued a "cookie", particularly when they retain sole control of compliance with its purpose or retention period. In respect of the obligations incumbent on the website publisher in such cases, the obligation to ensure with its partners that they do not issue, through its website, "cookies" that do not comply with the regulations applicable in France and that of taking any useful steps with them to put an end to breaches*" (see also CNIL, FR, 27 September 2021, Sanction, [REDACTED] Company, No. SAN-2021-013, published).
83. The restricted committee also notes that while the recommendations issued by the Commission on cookies have recently evolved to take into account the developments induced by the GDPR in terms of consent, in particular, these changes have no impact in this case and it has been continuously considered, as indicated in deliberation No. 2013-378 of 5 December 2013 adopting a recommendation on cookies and other trackers referred to in Article 32-II of the Act of 6 January 1978, since repealed, that "*when several players intervene in the storage and reading of cookies (for example when publishers facilitate the deposit of cookies which are then read by advertising agencies), each of them must be considered as jointly responsible for the obligations arising from the provisions of the aforementioned Article 32-II [current Article 82 of the Act of 6 January 1978]*". This deliberation specifies that this is the case "*of publishers of websites (or mobile app publishers, for example) and their partners (advertising agencies, social networks, publishers of audience measurement solutions, etc.). Indeed, insofar as website publishers often constitute the sole point of contact for Internet users and that the deposit of third-party Cookies depends on browsing their website, it is their responsibility to proceed, alone or jointly with their partners, with the prior information and the collection of consent explained in Article 2 of this recommendation*". The restricted committee also states that it has already enshrined the responsibility of publishers of websites in several decisions (see on this point, Deliberation SAN-2021-013 of 27 July 2021).
84. The restricted committee notes that a reCaptcha mechanism, provided by Google, is used when creating an account on the mobile application as well as when logging in performing the

forgotten password procedure on the website. The restricted committee considers that it was indeed the publisher of the website - in this case [REDACTED] - who chose to use the reCaptcha mechanism and therefore allowed the actions of reading and writing data present on users' terminals.

85. In view of the foregoing, the restricted committee considers that the company is not justified in arguing that it is under no obligation or responsibility for the operations carried out by Google via reCaptcha aimed at accessing information already stored on users' electronic communications terminal equipment, or at recording data in this equipment without their consent when they visit its website. It therefore considers that the company is also responsible for compliance with the provisions of Article 82 of the French Data Protection Act when using Google's reCaptcha mechanism.
86. **Secondly**, the restricted committee considers that while a data controller can claim an exemption from information and collection of consent when the read/write operations performed on a user's terminal are for the sole purpose of securing an authentication mechanism for the benefit of users (see on this point CNIL, FR, 27 September 2021, Sanction, [REDACTED] Company, No. SAN-2021-013, published), the opposite is true when these operations also pursue other purposes that are not strictly necessary for the provision of a service. However, the purpose of the Google reCaptcha mechanism is not for the sole purpose of securing the authentication mechanism for the benefit of users but also allows analysis operations by Google, which Google itself specifies in its General Terms and Conditions of Use.
87. The restricted committee notes that GOOGLE informs companies using reCaptcha technology, under the General Terms and Conditions of Use available online, that the functioning of the reCAPTCHA API is based on the collection of hardware and software information (such as data on devices and applications) and that this data are transmitted to Google for analysis. GOOGLE also states that such companies are responsible for informing users and requesting their permission regarding the collection and sharing of data with GOOGLE.
88. In this case, it emerges from these elements that [REDACTED] should have informed users and obtain their consent, which is not the case here.
89. Whilst [REDACTED] informed users, within the framework of its privacy policy, that "*when you visit our Site or Application, browsing and location data from cookies or similar technologies will be collected.*", the precise purposes of the cookies used, the possibility of objecting to them or that the continuation of the visit constitutes a form of consent is not part of the information provided by the company. Thus the information, accessible via the privacy policy on the website was only provided after cookies and other trackers had been stored and in a non-specific manner, whereas the recommendation resulting from deliberation No. 2020-092 of 17 September 2020 clearly provided that the information should be specific and prior to said storage. Therefore it cannot be considered that users were informed and consent validly obtained in light of the recommendations of deliberation No. 2020-092 dated 17 September 2020.

90. **Lastly**, as concerns the enforceability of deliberation No. 2020-092 dated 17 September 2020 as concerns analysing the obtaining of users' consent, the restricted committee points out that deliberation No. 2020-092 for adopting a recommendation proposing practical compliance procedures in the event of the use of "cookies and other trackers" aims to interpret the applicable legislative provisions and to inform stakeholders on the implementation of concrete measures to ensure compliance with these provisions so that said stakeholders implement these measures or measures having an equivalent effect. On this point it is stated in the recommendations that they *"are primarily intended to recall and explain the law applicable to the reading and/or writing of data (hereinafter "trackers") on the subscriber's or user's (hereinafter "users") electronic communications terminal equipment"*.
91. The Commission pointed out, in the context of its recommendation of 17 September 2020, that "when none of the exceptions provided for in Article 82 of the French Data Protection Act applies, users must, on the one hand, receive information in accordance with this article, supplemented, where applicable, by the requirements of the GDPR, and, on the other hand, be notified of the consequences of their choice".
92. The rapporteur notes that the CNIL has not created in its recommendation new obligations incumbent on the stakeholders but merely illustrated in concrete terms how Article 82 of the law must be applied.
93. In this respect, the fact that the recommendation of 17 September 2020 would not be enforceable against the company, in view of the methods for obtaining consent applicable on the date of the audit, has no impact since Article 82 of the French Data Protection Act provides that *"any user of an electronic communications service must, unless it has been informed beforehand, be informed in a clear and complete manner by the data controller or its representative: 1. Of the purpose of any action aimed at electronically accessing information already stored on their electronic communications terminal equipment, or writing information to this equipment; 2. Of how said user can object to it"*.
94. However, the company did not inform users even regarding the provisions of the former recommendation resulting from deliberation No. 2013-378 of 5 December 2013, prior to the provisions of deliberation No. 2020-092, of the precise purpose of the cookies, the possibility of objecting to said cookies and that continuing browsing constitutes agreement to the storage of cookies on users' terminals.
95. **Finally**, the restricted committee notes that [REDACTED] intends not to use this mechanism after October 2022. However, at the date of the controls, the mechanism was indeed used.
96. Therefore in view of the foregoing, the restricted committee considers that the company breached its obligations under Article 82 of the French Data Protection Act by allowing the placing of cookies on user terminals via the reCaptcha mechanism provided by Google without informing users and without obtaining their consent.

III. On corrective measures and publicity

97. Under the terms of Article 20 III of the amended Act of 6 January 1978:

“When the controller or its subcontractor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL’s Restricted Committee with a view to the imposition, after proceedings in which both sides are represented, of one or more of the following measures: [...]”

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83”.

98. Article 83 of the GDPR states that “*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive*”, before specifying the information to be taken into account when deciding whether to impose an administrative fine and when deciding on the value of such fine.

99. **Firstly**, the Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in Article 83 of the GDPR such as the nature, gravity and duration of the infringement, the measures taken by the data controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the infringement.

100. The restricted committee first considers that the company is guilty of serious failures in terms of the protection of personal data since breaches of fundamental and basic principles of the GDPR and the French Data Protection Act are constituted, such as the principles of data minimisation and the obtaining of users' consent before registering and reading information on its electronic communication terminal equipment.

101. The Restricted Committee then notes that the infringement of the rights of individuals resulting from the breach of the principle of minimisation of personal data is particularly important, given the special nature of geolocation data. Indeed, the company undertakes near-permanent geolocation data collection from users of the scooters it rents. Such data collection is particularly intrusive for users. In fact, it makes it possible to track all of the journeys made by users and identify the places they go to, thereby possibly revealing information about their behaviour and their life habits, which is likely to infringe their freedom of movement and privacy.

102. The Restricted Committee also points out that the personal data processed by the company concerns about [REDACTED] users distributed over the territory of three Member States of the European Union.
103. The restricted committee also notes that certain contracts entered into by [REDACTED] with its subcontractors are incomplete and do not contain all the information provided for in Article 28(3) of the GDPR or do not provide for sufficiently precise obligations incumbent on the subcontractor.
104. Regarding the reCaptcha mechanism, the restricted committee considers that the breach of Article 82 of the French Data Protection Act is characterised by the fact that the company has not complied with the requirements for information and obtaining consent, which has had the effect of depriving users of the choice they must be able to express as to the terms under which their personal data will be used.
105. Consequently, the restricted committee considers that an administrative fine should be imposed regarding the breaches constituted by Articles 5(1)(c) and 28(3) of the GDPR and Article 82 of Act No 78-17 of 6 January 1978 on data processing, files and freedoms as amended.
106. **Secondly**, as regards the value of the fine, the Restricted Committee recalls that administrative fines must be effective, proportionate and dissuasive.
107. In this case, the company breached its obligations under Articles 5(1)(c) and 28(3) of the GDPR and Article 82 of Act No. 78-17 of 6 January 1978 on data processing, files and freedoms as amended regarding approximately [REDACTED] users.
108. However, the restricted committee takes into account the fact that, at the end of the inspections carried out by the CNIL delegation, the company complied with the contracts entered into with [REDACTED] and [REDACTED] regarding the requirements of Article 28(3) of the GDPR.
109. In particular, it considers that the organisation's activity and financial situation must be taken into account when determining the sanction and, in particular, in the case of an administrative fine, its value. It points out in this respect that in 2019 the company generated revenue of [REDACTED] for a net loss of [REDACTED]. The company estimated its turnover for the financial year ended 31 December 2020 at [REDACTED] and a loss of [REDACTED].
110. Therefore in view of these facts, the restricted committee considers that the imposition of an administrative fine of 100,000 euros for breaches of the GDPR and 25,000 euros for the breach of the French Data Protection Act would appear justified.
111. **Thirdly**, the restricted committee considers that the publication of the sanction is justified in view of the particular nature of the data concerned which relates to geolocation data and the breach of users' privacy.

FOR THESE REASONS

The CNIL's restricted committee, after having deliberated, decides to:

- impose an administrative fine of 100,000 (one hundred thousand) euros against [REDACTED] in respect of the breaches constituted by Articles 5(1)(c) and 28(3) of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of personal data and the free movement of such data, and 25,000 (twenty-five thousand) euros regarding the breach constituted by Article 82 of modified Act No. 78-17 of 6 January 1978 on information technology, files and freedoms;
- publish its decision on the CNIL and Légifrance websites, which will no longer identify the [REDACTED] company by name at the end of a two-year period following its publication.

The Chair

Alexandre Linden

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

The President



Paris, on July 24, 2024

Our ref.: [REDACTED]

To be stated in all correspondence

Recorded delivery letter N° [REDACTED]

Dear Sir

The main activity of the company [REDACTED] is the sale of wines online in the form of public auctions via its website. It offers its services mainly in France and in several European Union countries. It has nearly [REDACTED] customers accounts in Belgium, nearly [REDACTED] in Germany and nearly [REDACTED] in Italy.

In accordance with **decision No 2023-192C of 26 June 2023**, on 23 August 2023 the Commission Nationale de l'Informatique et des Libertés (CNIL) carried out an online inspection of the website accessible at the URL “[REDACTED]” published by [REDACTED].

The purpose of this inspection was to verify the compliance of the processing implemented by your company with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on data protection (GDPR) and Law No 78-17 of 6 January 1978 as amended. In particular, the purpose of this inspection was to investigate a complaint lodged with the CNIL concerning the use of cookies in the user's terminal before any action being taken when browsing the ‘[REDACTED]’ website, as well as the incomplete and inaccessible nature of the information required by GDPR.

The findings made during this inspection, as well as the additional information provided on 22 September 2023, lead me to raise the following points.

I. Analysis of the facts in question

1. Regarding the breach of the obligation to define and comply with a retention period proportionate to the purpose of the processing operation

Article 5(1)(e) GDPR states that personal data must be “*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [...]*”.

In the specific case of the retention of data linked to a user account created on a website, this can in principle be retained until the account is deleted.

RÉPUBLIQUE FRANÇAISE

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

However, users often stop using these accounts without deleting them, which means that they continue to exist indefinitely. In this case, the principle of limited retention of personal data requires the controller to determine a reasonable period of time after which, if there has been no activity on the part of the user, the account must be considered as inactive and must be deleted, along with the personal data linked to it.

In this respect, the CNIL considers, in its reference framework relating to personal data implemented for the purposes of managing commercial activities,¹ that a period of two years is generally proportionate. It is advisable to warn the users concerned before deleting the accounts of those who have not reacted within the time limit set by the organisation.

In this case, the delegation was informed that data relating to non-customer members is kept indefinitely so that they can access the free services they have requested (access to wine quotations, cellar creation tools, receipt of wine alert emails, etc.). The data is thus retained as long as the member does not delete the account created, regardless of its use. The delegation was informed that this data is not used for commercial purposes.

I therefore consider that [REDACTED] has breached the provisions of Article 5(1)(e) of the GDPR by retaining for an unlimited period the data relating to non-customer members no longer using the services offered by the company.

2. On the breach of the obligation of transparency and to provide information to individuals

In law, Article 12(1) GDPR provides that “*the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language*”.

By way of illustration, the Article 29 Working Party (known as the “G29” and now the European Data Protection Board, EDPB) states, in its guidelines of 11 April 2018 on transparency within the meaning of Regulation (EU) 2016/679, that the criterion “*easily accessible means that the data subject should not have to search for the information but should be able to access it straight away*” and that “*An overriding aspect of the principle of transparency [...] is that the data subject should be able to determine in advance what the scope and consequences of the processing operation include so as not to be taken by surprise*”. It recommends as a matter of good practice that “*in an online context, a link to the privacy statement or notice should be provided at the point of collection of the personal data, or that this information should be available on the same page where the personal data is collected*”.

The guidelines also state that the information “*should be clearly differentiated from other non-privacy related information such as contractual clauses or general terms of use*”. The guidelines also state that “*the data subject should not have to actively search for the information covered by [Articles 13 and 14] among other information such as the terms of use of a site [...]*”.

¹ https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf

In this respect, the Commission considers that the information provided to data subjects does not appear on a separate medium from the legal notice and general terms and conditions, but is only accessible via links entitled “General terms and conditions” or “Legal notice”, inserted at the foot of personal data collection forms placed online on a website, and does not enable users to benefit from sufficiently clear and accessible information on the processing of their data. This method of providing information to data subjects does not meet the transparency and accessibility requirements laid down by GDPR. (CNIL, P, 1 December 2021, Formal notice, Company X, No MED-2021-131, unpublished)².

Article 13 GDPR requires the controller to provide the data subject with various items of information, in particular regarding the identity and contact details of the controller, the purposes of the processing carried out, its legal basis, the recipients or categories of recipients of the data, and whether the controller intends to transfer data to a third country. The Regulation also requires that, where it appears necessary to ensure *“fair and transparent processing”* of personal data, that individuals are informed about the period of data retention, the existence of the various rights entitled by individuals, the existence of the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority.

In this case, the delegation noted that the creation of a member account is mandatory to buy or sell products on the website “██████████”. To do so, the user is asked to complete a form, displayed in a pop-up window, including his/her name and email address, and he/she is asked to tick a box to accept the “General Terms and Conditions of Services” (CGS).

The delegation noted that a clickable hyperlink on the term "CGS" sends the internet user to a page that contains several drop-down sections. By clicking on the “Legal notice” section, the user can access the page dedicated to the protection of personal data by clicking on a new very light grey hyperlink.

Furthermore, the delegation noted that said data protection policy contained the majority of the mandatory information set forth in Article 13 GDPR with the exception of that relating to the legal bases of processing and data retention periods.

Finally, following the inspection, the company indicated that it had set up a link on its website entitled “Personal Data”, referring to the page containing the data protection policy, which was not present during the online inspection. Informal checks have confirmed the effectiveness of this change.

It follows from all the foregoing that information relating to the protection of personal data is not easily accessible for users of the website “██████████” when collecting their data for the creation of an account, as they must actively search for this information among the general terms and conditions of service and carry out multiple actions to be able to access it.

In addition, it appears from the findings made that this information does not specify the legal basis for each processing carried out. Furthermore, information on the data retention period is not mentioned, which in this case does not guarantee fair and transparent processing of individuals’ data.

² See “Table et informatique” (https://www.cnil.fr/sites/cnil/files/202312/tables_informatique_et_libertes.pdf).

I therefore consider that [REDACTED] has breached the provisions of Articles 12 and 13 of GDPR by not providing complete, transparent and easily accessible information to users of the website [REDACTED].

3. On the breach of the obligations relating to the joint processing liability

In law, Article 26(1) GDPR provides, in the event of joint processing responsibility, the definition by agreement or in a text of national or Union law of the respective obligations of joint controllers for the purpose of ensuring compliance with GDPR requirements. Article 26(2) requires that the broad outlines of this agreement be communicated to the data subjects.

In this case, the delegation was informed that [REDACTED] and [REDACTED] [REDACTED] are jointly responsible for the processing intended to manage buyer and seller customers at auctions. A service agreement dated 3 July 2023 governs the contractual relationship between these two companies. The delegation also noted that the personal data protection policy does not contain any information on the existence of joint responsibility. The general terms and conditions of the services posted online on the “[REDACTED]” website specify the services provided respectively by each of these companies.

However, it appears that the partnership agreement does not define the respective obligations of joint controllers for the purpose of ensuring compliance with GDPR. In addition, no information relating to their respective roles in this processing and their relations with the data subjects is communicated to them.

I therefore consider that [REDACTED] has breached the provisions of Article 26 GDPR.

4. On the breach of the obligation to inform the data subjects and obtain their prior consent before registering information on their electronic communications terminal equipment or accessing it (cookies and other trackers)

In law, Article 82 of the French Data Protection Act provides that “*Any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he/she has been informed in advance, by the controller or its representative, of:*

1° The purpose of any action to access, by electronic transmission, information already stored in his/her electronic communications terminal equipment, or to write information into that equipment;

2° The means available to him/her to oppose such action.

Such access or registration may only take place if the subscriber or user has expressed, after receiving this information, his/her consent, which may result from the appropriate settings of his/her connection device or any other device under his/her control [...].”

Paragraph 3 of this article sets out exceptions to this obligation for operations whose sole purpose is to enable or facilitate communication by electronic means, or which are strictly necessary for the provision of an online communication service at the express request of the user.

Article 4(11) GDPR defines “consent” 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”.

In this case, during the online inspection of the “[REDACTED]” website, the delegation noted, when accessing the website and before any action, the deposit of 17 cookies in the browser of the terminal used to carry out the inspection, including Google Analytics, DoubleClick and Adsense cookies. The delegation was informed that the DoubleClick and Adsense cookies have an advertising purpose and that the Google Analytics cookie has an audience measurement purpose. For the latter, it was specified that your company had chosen to no longer use the Google Analytics audience measurement solution.

The delegation also noted, upon arrival on the site’s home page, the presence of an information banner which specified that cookies “allow us to personalise the presentation of our wine selections, according to your preferences and your browsing history” accompanied by two buttons - “I configure my choices” and “I accept” - and a link “I continue without accepting”, located at the top right of the information banner.

Finally, informal findings show that, from now on, eight cookies are placed in the user’s browser as soon as they arrive on the home page and before any action. The DoubleClick, AdSense and Google Analytics cookies are no longer among the cookies placed.

However, in view of all of these factors, I note first of all that cookies not exempt from consent - because they pursue an advertising purpose - were placed on the browser of the users’ terminal without their prior consent.

Then, the cookies of the Google Analytics solution could not benefit from an exemption from the requirement of Article 82(2) of the French Data Protection Act. Indeed, they are not essential for the provision of an online communication service at the express request of the user and, due to their inclusion in the targeted advertising system implemented by Google, they combine this purpose, at least, with that of measuring the audience on the company’s website. Therefore, their storage was subject to the prior consent of the users.

Finally, the information banner relating to cookies does not comply with the minimum requirements allowing the collection of sufficiently informed prior consent and in accordance with Article 82 of the French Data Protection Act in that it does not inform the data subjects of the advertising purpose pursued by the storage of cookies.

I therefore consider that [REDACTED] breached the obligations of Article 82 of the Law of 6 January 1978 as amended.

I also draw your attention to the fact that, in the event that the measurement solution now used by [REDACTED] allows individual monitoring of the user, it could not benefit from the exemptions to consent set forth in Article 82 of the French Data Protection Act. For all practical purposes, I invite you to read the fact sheet published on the CNIL website “Cookies: solutions for audience measurement tools”.³

³ <https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience>

II. Corrective measures ordered by the CNIL (Article 20.II of the Act of 6 January 1978)

Due to all these elements, and in agreement with the other data protection authorities concerned by this processing operation, the following corrective measures should therefore be taken against [REDACTED]

- 1. A REMINDER OF LEGAL OBLIGATIONS**, in accordance with the provisions of Article 20.II of the Law of 6 January 1978, with regard to the obligation to obtain consent from individuals to register information on their terminal equipment (cookies) and to access them (Article 82 of the French Data Protection Act).
- 2. FORMAL NOTICE** in accordance with the provisions of Article 20.II of the Law of 6 January 1978, within **three (3) months of notification of this decision and subject to any measures it may have already adopted**, to:
 - **define and implement a retention period policy** for data from inactive accounts of non-customer members that does not exceed the period necessary for the purposes for which it was collected, in accordance with Article 5(1)(e) GDPR, unless it is justified in order to meet a legal obligation or for evidential purposes;
 - **inform data subjects**, in accordance with the provisions of Articles 12 and 13 GDPR, by providing them with complete, transparent and easily accessible information, in particular by completing the “Personal Data” policy posted on the [REDACTED] website and by referring them to it from the account creation form;
 - **define the respective obligations of the joint controllers** by means of an agreement and make the outline of this agreement available to the data subjects, in accordance with Article 26 GDPR;
 - **inform individuals of all the purposes pursued by the use of cookies** when browsing the [REDACTED] website, in particular by supplementing the information already present on the “cookies” banner by mentioning the advertising purpose pursued by them.

This decision, which does not require a response from you, entails the closure of procedure No 2023-092C. However, this closure takes place without prejudice to the Commission's right to carry out a new inspection in order to verify that your company has adopted the required measures at the end of the given period.

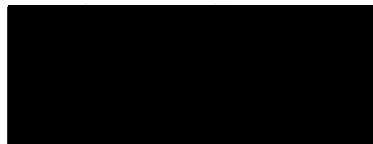
In the event of a new verification procedure, if your company has not complied with this formal notice, a Rapporteur will be appointed who may ask the Restricted Committee to impose one of the penalties set forth in Article 20 of the Law of 6 January 1978.

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

For more information on the formal notice procedure, you can consult the CNIL website at:
<https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0>.

The CNIL's departments ([REDACTED], Legal Officer in the Inspections Department,
[REDACTED] and [REDACTED] Information Systems Auditor in the Inspections
Department ([REDACTED]) are at your disposal for any further information you
may require.

Sincerely



Marie-Laure Denis

Registered letter with acknowledgement of receipt

No. AR: [REDACTED]

[REDACTED]
For the attention of the president

File processing:

Paris, on

08 AOUT 2024

Ref: [REDACTED]

Complaint No. [REDACTED]

(to be included in all correspondence)

Mr president,

I am following up on the e-mail exchanges that have taken place between the services of the Commission Nationale de l'Informatique et des Libertés (CNIL) and [REDACTED]'s data protection officer, as part of the investigation of Mr [REDACTED]'s complaint forwarded by the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*), in application of the mechanism for cooperation between European authorities pursuant to Articles 56 et seq. of the General Data Protection Regulation (GDPR).

As a reminder, the complainant lodged a complaint about the difficulties encountered in obtaining the erasure of all the personal data concerning him processed by your company.

Discussions between the CNIL and [REDACTED]'s data protection officer, by letters of 15th June and 13th July 2021, revealed the following.

With regard to the first request made by the complainant, you stated that the lack of response to this request was due to the fact that the contact address [REDACTED] which appeared on the [REDACTED] website and had been used by the complainant was in fact incorrect.

However, you indicated that in order to avoid this situation, a correction had been made on the website in question to direct users to the contact address [REDACTED] in the section « Who should I contact in the event of a complaint? » and to the [REDACTED]'s data protection officer for France ([REDACTED]), Belgium ([REDACTED]), Italy ([REDACTED]), Portugal ([REDACTED]) and Spain ([REDACTED]).

RÉPUBLIQUE FRANÇAISE

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

With regard to the complainant's second request for erasure, although the company initially warned him that it would have recourse to the extension of the deadline provided for in Article 12 in order to process the request, the company did reply. The complainant was then informed that the company was obliged to retain his personal data for evidential purposes for a period of 5 years from the termination of the contract (in this case, on 17th January 2020), pursuant to the provisions of article L110-4 of the French Commercial Code and article 17.3.b) of the General Data Protection Regulation.

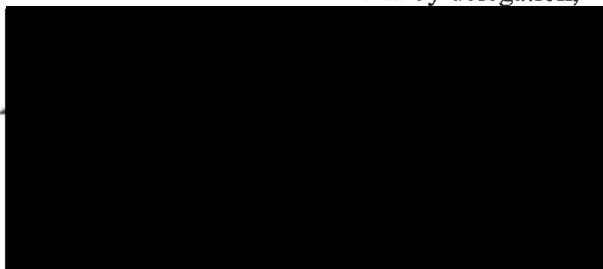
However, I note that the company proceeded on 4th March 2020 to erase the complainant's data that could have been deleted, in particular his bank details, including his IBAN, and that measures have since been taken to ensure that the complainant's personal data are no longer used for canvassing purposes. I also note that your company has taken due note of its obligations under the provisions of Article 12 in particular, in order to prevent such a situation from recurring.

In view of all these factors, and in agreement with the other European data protection authorities concerned, I am closing this complaint.

In the event of further complaints, the CNIL reserves the right to use all the powers granted to it by the GDPR and the amended Act of 6th January 1978.

Yours sincerely

For the President of the CNIL and by delegation,

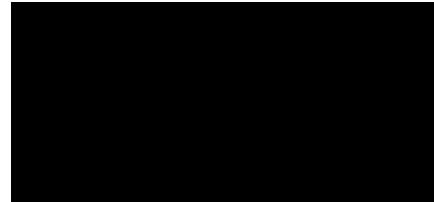


Subject to the applicant's right to bring an action, CNIL decisions may be appealed to the Conseil d'Etat within two months of their notification, extended by :

- one month for residents of Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, Mayotte, Saint-Pierre-et-Miquelon, French Polynesia, the Wallis and Futuna Islands, New Caledonia and the French Southern and Antarctic Territories;*
- two months for people living abroad.*

Registered letter with acknowledgement of receipt

No. AR : [REDACTED]



File processing:

Paris, on

N/Ref.: [REDACTED]

Complaint No. [REDACTED]

(to be included in all correspondence)

Mr president,

I am following up on the e-mail exchanges that have taken place between the services of the Commission Nationale de l'Informatique et des Libertés (CNIL) and [REDACTED]'s data protection officer, as part of the investigation of Mr [REDACTED]'s complaint forwarded by the German Data Protection Authority of the Land of Berlin (*Der Berliner Beauftragte für Datenschutz und Informationsfreiheit*), in application of the mechanism for cooperation between European authorities pursuant to Articles 56 et seq. of the General Data Protection Regulation (GDPR).

As a reminder, the complainant lodged a complaint against the company [REDACTED] relating to a security and confidentiality issue in the processing of his personal data. On 19th September 2019, the complainant indicated that he had received an e-mail from [REDACTED] on his e-mail address ([REDACTED]), giving the surname, first name, telephone number and e-mail address of a third party.

In the exchanges that took place between the CNIL services and [REDACTED]'s data protection officer, by e-mails of 26th November and 18th December 2020, it was indicated that this disclosure of personal data would be the consequence of an internal human error.

It was specified that following the intervention of the CNIL services in the case of such a disclosure, [REDACTED] notified the personal data breach to the data subject.

These facts lead me to remind you that, it is your responsibility as data controller to:

- ensure compliance with Article 5(1)(a) of the DGPD, by ensuring that personal data are processed lawfully, fairly and in a transparent manner ;

RÉPUBLIQUE FRANÇAISE

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

- implement, taking into account the nature, scope, context and purposes of the processing, as well as the varying degrees of risk to the rights and freedoms of natural persons, the appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Article 24(1) of the GDPR ;
- in the event of a personal data breach, to notify the CNIL of the breach without undue delay and, if possible, no later than 72 hours after having become aware of it in accordance with Article 33 of the GDPR. As part of its security obligations, the data controller shall set up a procedure to manage personal data breaches, with the aim of preventing, detecting and reacting appropriately to limit the risks and avoid future breaches.

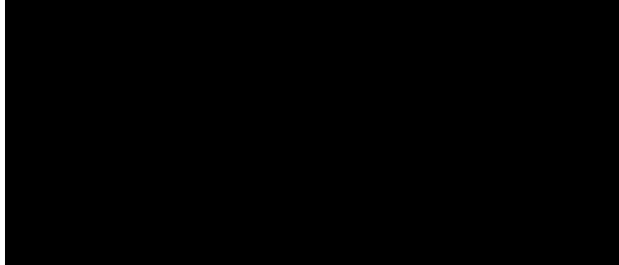
You will find more information on these subjects on the CNIL website:

- o <https://www.cnil.fr/fr/les-violations-de-donnees-personnelles>
- o <https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles>

**Given the answers provided and the measures adopted, and having no doubt that [REDACTED]
has since taken the necessary measures to ensure the security of its processings, in agreement
with the other European data protection authorities concerned, I hereby inform you that I am
closing this complaint.**

In the event of further complaints, the CNIL reserves the right to use all the powers granted to it by the GDPR and the amended Act of 6th January 1978.

Yours sincerely

For the President of the CNIL and by delegation,


Subject to the applicant's right to bring an action, CNIL decisions may be appealed to the Conseil d'Etat within two months of their notification, extended by:

- one month for residents of Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, Mayotte, Saint-Pierre-et-Miquelon, French Polynesia, the Wallis and Futuna Islands, New Caledonia and the French Southern and Antarctic Territories;
- two months for people living abroad.

A/R ref. [REDACTED]

File processing:

2024 [REDACTED]

N/Ref :

Referral N°

(to be included in all correspondence)

Paris, 7 August

Dear Madam,

You have lodged a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL) against Mr [REDACTED].be website (hereinafter "████████"), concerning the difficulties encountered in exercising your right to the deletion of your personal data.

On 28 September 2021, you contacted the publisher of the [REDACTED] website to request, on the basis of Article 17 of the GDPR, the deletion of your personal data from the [REDACTED] website relating to remuneration for your professional activity with [REDACTED]. You stated that the data in question related to your private professional activity as an employee and that, in your opinion, there were no compelling legitimate grounds for continuing to process this data. You therefore also objected to the processing of this data for reasons relating to your particular situation. You subsequently extended your request for erasure to all information relating to your earnings as an employee in the private sector between 2018 and 2020.

On 18 October 2021, the publisher of the [REDACTED] website refused to grant your request on the grounds that the publication of this information on its website contributes to the transparency that is essential for the proper functioning of democracy with regard to the allocation of certain mandates, functions and professions. The publisher of the [REDACTED] site pointed out that the information on its site was taken from public and official sources and stated that you were subject to the obligation to declare your mandates and remuneration under the *law of 2 May 1995 relating to the obligation to file a list of mandates, functions and professions and a declaration of assets*.

As you know, in application of the mechanisms for cooperation between authorities provided for by the General Data Protection Regulation (GDPR), the CNIL has forwarded your complaint to the Belgian data protection authority (hereinafter "*Belgian authority*"), which is competent to deal with requests relating to [REDACTED] insofar as the data controller is established in Belgium.

On 13 June 2022, the Litigation Division of the Belgian authority decided that this case could be dealt with on its merits. As a result, you have had several opportunities to discuss your case with the Litigation Division of the Belgian authority and to put forward your arguments. The same was true for the publisher of the [REDACTED] website.

RÉPUBLIQUE FRANÇAISE

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

Following these exchanges, and pursuant to Article 77 of the General Data Protection Regulation (GDPR), I hereby inform you of the decision adopted in this matter. The CNIL is responsible for informing you of the decision taken, in accordance with articles 56.6, 60.7 and 60.8 of the GDPR.

By way of introduction, we inform you that under the terms of Article 17(1)(c) of the GDPR, the data subject has the right to obtain from the controller the erasure, as soon as possible, of personal data relating to him or her where "*(...) (c) the data subject objects to the processing pursuant to Article 21(1) and there are no compelling legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR*".

However, the right to protection of personal data is not an absolute right; it must be balanced against other fundamental rights. In this respect, publications on the web fall within those protected by the right to freedom of expression and information (Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Article 11 of the EU Charter of Fundamental Rights).

Article 17(3)(a) of the GDPR provides that Article 17(1) shall not apply insofar as processing is necessary for the exercise of the right to freedom of expression and information, thus providing, in the very terms of Article 17 of the GDPR, for a system of exceptions which involves a balancing of the fundamental right to freedom of expression and information on the one hand and the fundamental right to the protection of personal data on the other.

In the course of its case law, the European Court of Human Rights (hereinafter "ECHR") has developed a series of relevant criteria that must be taken into account when balancing competing fundamental rights, namely the contribution to a debate of general interest, the reputation of the person concerned, the subject-matter of the report, the previous conduct of the person concerned, the content, form and impact of the publication, the manner and circumstances in which the information was obtained and its truthfulness.

Furthermore, the ECHR has regularly emphasised in its case law the indispensable role of the press, pointing out that its main function is to disseminate debates of general interest and that it also fulfils a secondary role, that of revealing and bringing to the attention of the public information likely to arouse interest and give rise to such a debate within society.

While in the case law of the ECHR, this role is generally played by the press and professional journalists, the Court is gradually recognising this function for private individuals. The Court considers that the role of these actors may be similar in importance to that of the press and that they may therefore benefit from the high level of protection usually afforded to the press.

Similarly, the CJEU gives a broad interpretation to concepts related to freedom of expression, such as journalism. In its "*Buivids*" judgment of 14 February 2019, the CJEU does not lay down any requirement as to the professional capacity of the person or organisation invoking the benefit of the journalistic exception. In particular, the purpose of the publication must be that of a journalist inspired by the public interest.

An analysis of the case law of the CJEU and the ECHR clearly shows that the exercise of an activity of a journalistic nature, and the resulting protection, should not be reserved exclusively for professional journalists. However, this same analysis also reveals that anyone who engages in journalistic activity and intends to benefit from the high level of protection afforded to freedom of the press is required to respect at least the most obvious rules of ethics.

In the light of these introductory remarks on the applicable case law and regulations, the Belgian authority took its decision on the basis of the following elements.

Firstly, the disputed processing essentially consists of the retranscription on [REDACTED] of your publicly available declarations of mandates and remunerations. In fact, you have held two mandates subject to the obligation to declare your mandates and remuneration under *the law of 2 May 1995 relating to the obligation to file a list of mandates, functions and professions and a declaration of assets*, so that your remuneration has been published in the *Moniteur belge* and on the website of the Court of Audit pursuant to this legal obligation.

Secondly, you are subject to this declaration obligation because you have held, and still hold, two senior management positions with a company that is essentially owned by the Belgian and French States. However, the *Act of 14 October 2018 amending the legislation on declarations of mandates and assets with regard to transparency of remuneration, extension to public directors, electronic filing and control*, extended the obligation to declare to so-called "public" directors who exercise certain functions with companies over which one or more public authorities exercise a dominant influence.

Thirdly, [REDACTED] argued that the purpose of publishing your remuneration is the same as that intended by the legislator through the laws governing the obligation to declare and publish mandates and remuneration. The publication of the information at issue does not serve any purpose other than that for which it was initially collected by virtue of the legal obligation to which the complainant is subject, in this case for the purposes of transparency in public management.

Fourthly, your request for deletion was not addressed to an established newspaper, but to publications on a citizens' website run by a person who is not a professional journalist. However, the processing at issue was carried out for journalistic purposes within the meaning of the aforementioned case law of the CJEU and the ECHR. [REDACTED] made your earnings available free of charge on its website in order to inform the public and draw its attention to the issue of public interest. The sole purpose of this processing is to inform the public about these issues of public interest. It also appears that [REDACTED] has respected certain essential rules of journalistic ethics by verifying and, where necessary, correcting the information it relays from official and public sources.

Fifthly, exercising your right to erasure relates to the processing of information that contributes to this debate of general interest and is therefore of interest to the public. The public interest in having this information is all the more important insofar as you are a public figure subject to the aforementioned obligation to declare, and play a role in Belgian public life.

Sixthly, the objective of transparency in public management pursued by [REDACTED] and *a fortiori* by the legislator when he adopted the aforementioned laws, requires that all types of remuneration, whether public or private, be accessible to the public. It appears that only the ranges of your private remuneration are published on [REDACTED]. The public interest in having access to the disputed information is to highlight, in particular, a possible conflict of interest. While it is true that publication of the functions performed would already expose a conflict of interest to a certain extent, in this context, publication of the ranges of other remuneration you receive as a public administrator is not disproportionate. In fact, it allows the public to form a more complete picture of potential conflicts of interest and to make relevant comparisons between private and public income.

Seventhly, the information at issue is not particularly sensitive and its dissemination by [REDACTED] does not have any significant repercussions, particularly as it is already publicly available and has, moreover, been actively communicated by yourselves in order to fulfil your obligations; you therefore could not have been unaware that this information was intended to be published by the Court of Auditors. While publication on [REDACTED] may create additional risks in comparison with official publication insofar as the scope of this

In this case, the risks are limited and would not justify restricting the legitimate rights of third parties to access this information in the public interest.

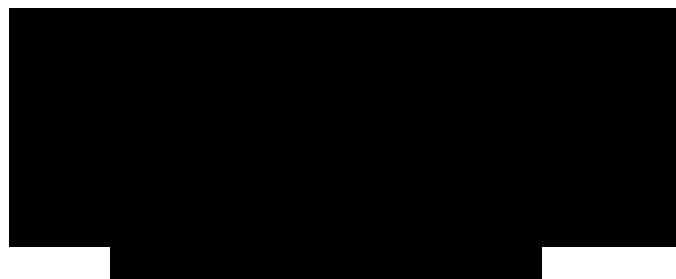
Finally, given that the information relayed on the [REDACTED] website comes from official sources and that you yourself are the source of this information, the accuracy of the disputed information is not called into question. It has been noted that the disputed information is recent and therefore still relevant, since it refers to professional activities that you have been carrying out since [REDACTED]

In the light of all these factors, the Belgian authority noted that the [REDACTED] website, by relaying and bringing together the disputed information in such a way as to make it more accessible to the public than official sources, was participating in a debate of public interest on the issue of transparency in public management and the fight against conflicts of interest and corruption and that, consequently, the publication on this site of your remuneration as an employee in the private sector appeared necessary for the exercise of the right to freedom of expression and information pursuant to Article 17.3. a) of the GDPR.

Consequently, and in accordance with the provisions of Article 17 of the GDPR, I hereby inform you that, in agreement with the European data protection authorities, your complaint has been rejected.

We would like to inform you that the Belgian authority considers this case to be important and intends to publish/replay the decision adopted on its website once your personal data has been deleted.

Yours faithfully

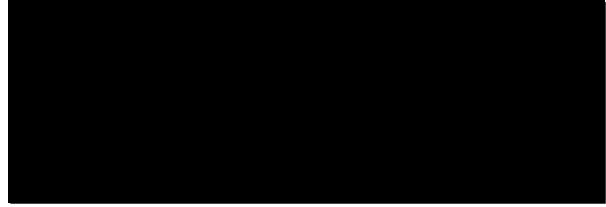


Subject to the applicant's right to bring an action, CNIL decisions may be appealed to the Conseil d'État within two months of their notification, increased :

- one month for residents of Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, Mayotte, Saint-Pierre-et-Miquelon, French Polynesia, the Wallis and Futuna Islands, New Caledonia and the French Southern and Antarctic Territories;*
- two months for people living abroad.*

Registered letter with acknowledgement of receipt

No. AR: [REDACTED]



File processing:

[REDACTED]
Paris, on 18th September 2024

Ref: [REDACTED]

Complaint No. [REDACTED]

(to be included in all correspondence)

Mr president,

I am following up on the exchanges that have taken place between the services of the Commission nationale de l'informatique et des libertés (CNIL) and those of [REDACTED], as part of the investigation of Mrs [REDACTED]'s complaint forwarded by the Spanish Data Protection Authority (*Agencia Española de Protección de Datos*), in application of the mechanism for cooperation between European authorities pursuant to Articles 56 et seq. of the General Data Protection Regulation (GDPR).

As a reminder, the complainant lodged a complaint against the company [REDACTED] regarding the unsolicited receipt of direct marketing mail at her postal address. The complainant claims that she had no contractual relationship with this company and that she did not provide any contact details.

In the first place, with regard to the source of the complainant's personal data, the exchanges that took place between the CNIL and [REDACTED] by letters of 30th November and 24th December 2021, revealed the following.

First of all, [REDACTED] points out that the complainant does not appear in its own customer database, insofar as she has never ordered products or taken part in the advertising games that enable the company to collect the personal data of prospective customers.

Furthermore, [REDACTED] states that it wished to canvass prospective customers. To do so, the company called on the services of [REDACTED], which rented out its database of prospective customers.

However, it appears that the complainant's personal data were included in the database of [REDACTED] insofar as the complainant, who has been a regular customer of [REDACTED] since 2012, consented in 2017 to the use of her personal data for direct marketing purposes by third-party partners, including [REDACTED]. A supporting document was provided by [REDACTED] to attest to its consent to receive direct marketing from partners of [REDACTED]

RÉPUBLIQUE FRANÇAISE

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

Lastly, [REDACTED] adds that it has contacted the complainant only once for direct marketing purposes.

In the second place, with regard to the complainant's right to object request, I take note that [REDACTED] states that it has stopped using her personal data for direct marketing purposes and has informed [REDACTED] accordingly.

In any event, in the future, I would draw your attention to the necessity for [REDACTED] to provide information to data subjects whose personal data are collected indirectly, in this case through its commercial partners, as soon as possible (in particular during the first contact with the person) and within one month at the latest.

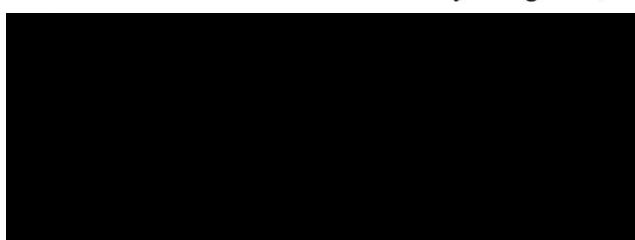
In this respect, in accordance with Article 14 of the GDPR, the identity and the contact details of the controller, the purposes of the processing, the categories of personal data concerned, the existence of a transfer of data to a recipient in a third country or an international organisation, the period for which the personal data will be stored, the rights of data subjects conferred by the GDPR, the right to lodge a complaint with a supervisory authority and the existence of automated decision-making must all be indicated. In addition, the source of the personal data collected must be indicated to the data subjects.

Given the answers provided and having no doubt that [REDACTED] has since taken the necessary measures to ensure the compliance of its processings, in agreement with the other European data protection authorities concerned, I hereby inform you that I am closing this complaint.

In the event of further complaints, the CNIL reserves the right to use all the powers granted to it by the GDPR and the amended Act of 6th January 1978.

Yours sincerely

For the President of the CNIL and by delegation,



Subject to the applicant's right to bring an action, CNIL decisions may be appealed to the Conseil d'Etat within two months of their notification, extended by:

- one month for residents of Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, Mayotte, Saint-Pierre-et-Miquelon, French Polynesia, the Wallis and Futuna Islands, New Caledonia and the French Southern and Antarctic Territories;

- two months for people living abroad.



Registered letter n° [REDACTED]

File processing:

Paris, 4th September 2024

N/Ref: [REDACTED]

Referral [REDACTED]

(to be included in all correspondence)

Dear Mr. [REDACTED],

I am writing further to the exchange of e-mails between the services of the Commission nationale de l'informatique et des libertés (hereinafter "the CNIL") and the Data Protection Officer of the [REDACTED] (hereinafter "the [REDACTED") as part of the investigation of the complaint sent to us by the personal data protection authority of the German federal state of Mecklenburg-Western Pomerania ("Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern"), pursuant to the provisions of Article 56.1 of the General Data Protection Regulation (hereinafter "GDPR").

This complaint concerned the difficulties encountered by Ms [REDACTED] in exercising her right of access to her personal data processed by [REDACTED].

The complainant stated that, in response to her request for access to a copy of her personal data, made by e-mail on 22 June 2023, she had received a reply by e-mail on 30 June 2023 containing, as an attachment, a document in PDF format containing personal data about her, including an unredacted copy of her identity card, transmitted unencrypted. This email was also sent to two people, in carbon copy, one apparently working for your institution, the other working as an Erasmus coordinator for the [REDACTED] (Mecklenburg-Western Pomerania).

The complainant argued that the reply she received should not have included a third party and that the copy of her identity document that she had provided should have been deleted no later than on the date on which the Erasmus exchange that had been planned with your organisation was cancelled.

She added that the data provided in response to her request seemed incomplete: in fact, as her correspondent within your organisation had told her that he wished to clarify a specific question concerning her internally, emails or, at the very least, internal notes or other elements, should have been processed or stored for this purpose and, consequently, included in the copy of her data sent. Finally, she pointed out that the copy did not contain all the information mentioned in Article 15(1) of the GDPR.

1. With regard to the retention of the complainant's identity document:

I have noted that the application process for an Erasmus exchange within your organisation includes the provision of a copy of the identity document, which has led, by deduction and habit, to this document being perceived as part of the application file. You indicate that the retention period for this element, for rejected applications, was set at one year, whereas in view of the intended purpose, the copy of the identity document should only be retained for the time necessary to verify the identity of the applicant and the accuracy of the data concerned, before being deleted. I have noted that your organisation's Data Protection Officer has asked the data controller (in this case, [REDACTED]'s [REDACTED] Department) to delete the copies of the identity cards concerned.

I would also point out that, if Ms [REDACTED]'s identity card was kept for longer than was strictly necessary, it would in any event have been deleted the following year.

2. With regard to the inclusion, in the above-mentioned e-mail of 30th June 2023, of two third parties :

I have taken note of the explanations given by your organisation's Data Protection Officer, according to which were carbon-copied in the response to Ms [REDACTED]'s request for access:

- 1) the Head of the [REDACTED] International Relations Department, for her information and follow-up of this request, by virtue of her function and, in this case, as data controller, as well as
- 2) the person responsible for coordinating the Erasmus programme at the complainant's home university.

In this respect, I also take note of the fact that, while the inclusion of the latter does indeed constitute an accidental transmission constituting a breach within the meaning of the GDPR, the degree of this breach remains low: firstly, the data concerned is used solely for academic purposes and does not constitute sensitive data, and secondly, the recipient is an agent responsible for managing the complainant's mobility in her home institution, bound by an obligation of discretion and professional secrecy in the performance of his duties and who does not constitute a "malicious actor".

Finally, I note that the CNIL was notified of this breach, following its intervention, and that the unauthorised recipient of the complainant's data was asked to delete the disputed email, which he confirmed in writing.

I have also noted that, since these exchanges, the staff concerned have been reminded of the need to involve the Data Protection Officer in all matters relating to data protection, including requests to exercise rights, in order to secure their processing, and a working meeting has been scheduled with the [REDACTED] Department to examine the precautions to be taken to avoid any similar incident.

I also note that the above-mentioned data breach did not have a significant effect on the data subject and is not one of the breaches likely to give rise to a risk or a high risk that must be notified to the Data Protection Authority (see [Guidelines 01/2021 on Examples of Personal Data Breach Notification adopted on 14 December 2021 in its version 2.0](#)).

3. Regarding the response to Ms [REDACTED]'s request for access:

I have noted that a further response was sent to the complainant by two emails dated 8 April 2024 which complied with the requirements of Article 15 of the GDPR and included a secure download link which enabled the complainant to download a copy of her personal data.

I would also point out that the complainant's request for access was initially partially dealt with within the time allowed.

In this context, the responses provided by [REDACTED] and the measures taken to respond to the complainant's request and to prevent a repetition of the facts that are the subject of her complaint lead me, in agreement with the other European Data Protection Authorities concerned by your processing operations, to close this complaint.

However, the CNIL reserves the right, in the event of further complaints, to make use of all the powers conferred on it by the provisions of the GDPR and Act no. 78-17 of 6th January 1978, as amended, relating to data processing, data files and individual liberties.

Yours sincerely,

For the Chair of the CNIL, and by delegation,

[REDACTED]
[REDACTED]



Case number: NAIH/2020/2305/

In charge: 

Re: Decision

DECISION

The Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter: Authority) brings the following decisions in its data protection procedure launched ex officio against  (registered office:  hereinafter: Obligee), in which the Authority investigated the compliance by the Obligee with the provisions of the General Data Protection Regulation (hereinafter: GDPR):

I. The Authority **establishes** that the Obligee acted unlawfully and infringed the provisions of GDPR, when it

- I.1. failed to make the information on its data processing easily accessible, thereby infringing Article 12(1) of GDPR;
- I.2. failed to take action within a month from the receipt of the access request, thereby infringing Article 12(3) of GDPR;
- I.3. failed to provide full information upon the access request, thereby infringing Article 15(1) of GDPR;
- I.4. made a photo recording of the identification document of the person making use of its accommodation service, thereby infringing Article 5(1)(c) of GDPR;
- I.5. uploaded the photo made of the identification document to the Obligee's WhatsApp group, thereby infringing Article 6(1) of GDPR.

II. The Authority **orders** the Obligee to

- II.1. make its information on data processing easily accessible on its website on the landing page, as well as in the course of reservation;
- II.2. provide the Customer information on the processing of his personal data, covering all the aspects of data processing in accordance with Article 15(1) of GDPR within 30 days from this decision becoming final.
- II.3. refrain from making photo recording of identification documents of its guests.

IV. The Authority imposes

**a data protection fine of
HUF 360,000, that is, three hundred and sixty-thousand forints**

because of the unlawful processing of data, payable within 30 days from this decision becoming final.

Obligee shall notify the Authority of the implementation of the measures set forth in Section II within 8 days from taking them, also enclosing the substantiating evidence.

The fine is to be paid to the targeted forint account of the Authority for the collection of centralised revenues (10032000-01040425-00000000 Centralised collection account IBAN: HU83 1003 2000 0104 0425 0000 0000). When transferring the amount, reference is to be made to this number: NAIH/2020/2305. BÍRS.

In the event that the Obligee fails to meet its obligation to pay the fine when due, it shall pay a penalty for delay. The rate of the penalty for delay is the legal interest rate corresponding to the central bank base rate quoted on the first day of the calendar half year affected by the delay.

In the event of a failure to meet the obligations according to Section II or the non-payment of the fine and a penalty for delay according to Section III, the Authority orders the execution of its decision.

There is no legal remedy against this decision through the administrative route, but it can be attacked in an administrative lawsuit through a petition addressed to the Fővárosi Törvényszék (Budapest Tribunal) within 30 days from its communication. The petition is to be submitted to the Authority electronically,¹ and the Authority will forward it together with the documents of the case to the Tribunal. For those who are not fully personally exempted from duty, the duty of an administrative lawsuit is HUF 30,000; the lawsuit is subject to the right of prenotation of duties. Legal representation is mandatory in a procedure in front of the Budapest Tribunal.

J U S T I F I C A T I O N

I. The course of the procedure

Based on the Client's complaint, the Berlin Data Protection Authority initiated a procedure to establish the lead supervisory authority and the other authorities concerned in accordance with Article 56 of GDPR through the IMI system under case number 63831 on 29 March 2019. The Client was unable to name the controller, it could pinpoint only its website, which is [REDACTED] (hereinafter: website).

Based on the website, the person of the controller could not be established as it did not display the name of the company operating the website, only its address ([REDACTED]) and the name of the managing director. According to public company information, no company providing accommodation services was registered to the address indicated in the website, but based on public company information, the Authority found a company called [REDACTED] whose registered offices are located at [REDACTED]
[REDACTED]

In view of the above, it was probable that the central operations of the presumed controller was in Hungary, so the Authority stated in the procedure according to Article 56 of GDPR that in its view the Authority is the lead supervisory authority in this case. After this, the Berlin Data Protection Authority sent the detailed complaint of the Client, his name and access data to the Authority on 31 May 2019.

The Authority launched an investigative procedure under case No. NAIH/2019/3239, of which it informed [REDACTED] at the address of [REDACTED] in a letter dated 27 June 2019 and called upon the company to answer the questions of the Authority with a view to clarifying the facts of the case. [REDACTED] received the Authority's letter on 8 July 2019. The Authority sent its letter also to the e-mail address displayed in the website [REDACTED] as well as to the mailing address indicated in the website: [REDACTED]. The Authority's letter sent to [REDACTED] was answered by [REDACTED] which had the same registered address as according to their statement, the Obligee was the controller in the case. The Obligee's statement was received by the Authority on 25 July 2019.

Simultaneously with contacting the undertaking presumed to be the controller, the Authority also contacted the Client, asking him to make his personal identification data and address available to the Authority and requested

¹ An administrative lawsuit can be initiated by using the form NAIH_K01: NAIH_K01 ürlap (16.09.2019) The form can be filled in using the general form fill-in program (ÁNYK program).

him that in the event that he received an answer to his access request from the controller since lodging the complaint with the Berlin Data Protection Authority, he should send it to the Authority. The Client's answer was received by the Authority on 31 July 2019.

In view of the fact that the Obligee failed to answer all the questions of the Authority the first time with respect to the processing of the Client's personal data, the Authority contacted the Obligee again on 12 December 2019. The Authority received the Obligee's statement on 30 December 2019 and it submitted additional evidence on 29 January 2020.

On 16 January 2020, the Authority informed both the Client and the Berlin Data Protection Authority that the procedure was still in progress.

On 4 March 2020, the Authority launched its data protection procedure ex officio in the case pursuant to Section 55(1)(ab) and Section 60(3)(b) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information (hereinafter: Privacy Act), of which it informed the Obligee on the same day, and called upon it to make statements in order to clarify the facts of the case.

The Obligee's statement was received by the Authority by e-mail on 26 March 2020 and on 31 March by mail.

Upon its request, the Authority informed the Berlin Data Protection Authority that the investigative procedure in the case was closed and the data protection procedure was launched on 31 March 2020.

II. The facts of the case

In his complaint lodged with the Berlin Data Protection Authority, the Client (his reservation numbers: 1681390; 2635357; 5376220) presented that he reserved accommodation through the website where he did not find information on data processing, so he was unable to study the Privacy Policy in advance.

When arriving at the accommodation on 3 November 2018, he and his companion had to fill in a form required for registration where they had to state their names, addresses, birth dates, the number of their identification documents, their e-mail addresses and phone numbers. After this, the employee of the landlord asked for the Client's identification document in order to make a photo of it using his smart phone. The Client first refused to do so, when the employee of the landlord informed him that in the absence of this, they will not be able to register and occupy the accommodation, so finally the photo was made of the identification document of his companion, which the employee uploaded to a group chat in WhatsApp.

On 7 November 2018, the Client submitted a request to access from the e-mail address [REDACTED] to the Obligee, in which he requested information on all his personal data processed by the Obligee on the basis of Article 15 of the General Data Protection Regulation (hereinafter: GDPR)². He also requested information on the forwarding of the data through WhatsApp, as well as the data storage in that application. On 8 November 2018, he received an answer from the e-mail address [REDACTED] informing him that his request was forwarded to the managing director, from whom he will get an answer within a few days. The Client did not receive any answer to his access request by 5 December 2018 when he sent his submission to the Berlin Data Protection Authority.

²Regulation (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 Client complained that no information on data processing was available in the website and that he did not receive an answer to his access request sent to the contact e-mail address of the landlord. He also objected to the fact that the employee of the landlord wished to make a photo of his identification document and that the employee of the landlord uploaded the photo of the identification document of his companion to the Obligee's WhatsApp group, which includes only a few employees of the Obligee and is used for sharing information in connection with the individual apartments rapidly.

Upon the first call of the Authority, the Obligee failed to give concrete answers concerning the Client, except for the screenshot of the registry concerning the Complainant and generally informed the Authority on data processing.

According to the Obligee's statement, guests are informed of its Privacy Policy available in the website [REDACTED] (hereinafter: Privacy Policy).

In the course of making the reservation, guests have to indicate that they accept the provisions of the Privacy Policy. The Obligee stated that the Privacy Policy is available to the guests in English and in Hungarian in every apartment.

In relation to the access request, the Obligee informed the Authority that it answered the request on 19 July 2019; the answer was delayed because of an administrative mistake. The copy of the answer was sent by the Obligee to the Authority.

The Obligee informed the Authority through his authorised representative that it only processes the name of the Client on the accounting voucher issued for him, the copy of which was sent to the Authority. The legal basis for processing the Client's name in the accounting voucher was Article 6(1)(c) of GDPR as Section 169(2) of Act C of 2000 on Accounting (hereinafter: Accounting Act) requires the Obligee to keep accounting vouchers for eight years. The purpose of data processing, i.e. keeping the accounting voucher, is to meet accounting obligations.

The Obligee supplemented its earlier statement stating that the delay in answering the access request of the Client took place because the employee handling incoming e-mails did not pay attention to it and he did not attach any significance to it. When GDPR became applicable, the Obligee developed an internal data processing protocol, provided training for the employees, still the omission took place on the part of the employees.

The Obligee deleted the photo made of the identification document of the Client's companion from the WhatsApp group; to substantiate this, it enclosed the screenshot of the chat in the WhatsApp group.

III. Applicable legal regulations

Pursuant to Article 2(1) of GDPR, GDPR is to be applied to data processing according to this case.

The provisions of GDPR relevant to this case are the following:

GDPT Article 5(1)(c): *Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimisation")*.

GDPR Article 12(1): *The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including where appropriate by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.*

GDPR Article 12(3): *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. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means, where possible, unless otherwise requested by the data subject.*

GDPR 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 data 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.*

Accounting Act Section 169(2): *The accounting vouchers (including general ledger accounts, analytical and detailed records) directly or indirectly substantiating bookkeeping shall be kept in a legible form, enabling their search based on references in the bookkeeping notes for at least eight years.*

GDPR Article 58(2)(b), (c) and (i): *Each supervisory authority shall have all of the following corrective powers:*

- b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this regulation;*
- c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this regulation;*
- i) to impose an administrative fine pursuant to Article 83, in addition to or instead of measures referred to in this paragraph depending on the circumstances of each individual case.*

GDPR 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.*

GDPR Article 83(1)-(2) and (5)(a)-(b): (1) *Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this article in respect of infringements of this Regulation referred to in paragraphs (4), (5) and (6) shall in each individual case be effective, proportionate and dissuasive.*

(2) *Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in point (a) to (h) and (j) of Article 58(2). 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 the 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 notify 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-*

(5) *Infringement of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher:*

- b) *the data subjects' rights pursuant to Articles 12 to 22.*

Privacy Act Section 2(2): *Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter: "General Data Protection Regulation") shall apply to the processing of personal data falling within the scope of the General Data Protection Regulation, with the additional rules laid down in Chapters III to V and VI/A, as well as in Section 3, points 3, 4, 6, 11, 12, 13, 16, 17, 21, 23 to 24, in Section 4 (5), Section 5 (3) to (5), (7) and (8), Section 13 (2), Section 23, Section 25, Section 25/G (3), (4) and (6), Section 25/H (2), Section 25/M (2), Section 25/N, Section 51/A (1), Sections 52 to 54, Section 55 (1) to (2), Sections 56 to 60, Section 60/A (1) to (3) and (6), Section 61 (1) a) and c), Section 61 (2) and (3), (4) b) and (6) to (10), sections 62 to 71, section 72, Section 75 (1) to (5), Section 75/A and Annex 1.*

Pursuant to Section 60(1) of the Privacy Act, to ensure that the right to the protection of personal data is enforced, the Authority may commence an administrative procedure for data protection ex officio. The rules of Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative Procedures Act) shall be applied to the data protection procedure of the Authority with the additions specified in the Privacy Act and the differences according to the General Data Protection Regulation.

Privacy Act Section 75/A: The Authority shall exercise its powers specified in Article 83(2) to (6) of the General Data Protection Regulation according to the principle of proportionality, in particular by primarily issuing, in compliance with Article 58 of the General Data Protection Regulation, a warning to the controller or processor for the purpose of remedying the infringement when the provisions laid down by law or a binding legal act of the European Union on the processing of personal data are first infringed.

The rules of Act CL of 2016 on General Administrative Procedures (hereinafter: Administrative Procedures Act) shall apply to the data protection procedure of the Authority with the additions specified in the Privacy Act and the differences according to the General Data Protection Regulation.

IV. The decision:

IV.1. Access to information

Article 12 of GDPR specifies the formal requirements which controllers must take into account when enabling the exercise of the rights of data subjects, including the provision of information in advance to data subjects. Accordingly, controllers must provide all information concerning the processing of personal data in a concise, transparent, intelligible and easily accessible form. This is supplemented by Article 13(1) of GDPR with the requirement that where personal data relating to a data subject are collected from the data subject, the controller shall inform the data subject of the circumstances of data processing at the time when the personal data are obtained.

According to the statement of the Client, he found no information concerning the processing of personal data on the website at the time of lodging his complaint.

Prior to launching the investigative procedure, the Authority checked the website of the Obligee where no page was found that would have contained the Privacy Policy or would have directed the viewer to it (screenshot: 2 April 2019, 18 June 2019).

In November 2019, the Authority examined the website of the Obligee again where there was a page entitled Policies; however under the Privacy Policy tab only some Latin sample text was found which was used for editing the website and not the Privacy Policy.

In November 2019 and also at the time of bringing this decision, the link pointing to the Privacy Policy became accessible when the guest or the future guest began reservation and chose the date of stay. In relation to the selected date, the website lists all the apartments, namely more than a hundred, that can be rented from the Obligee, irrespective of whether or not they are available and the link to the Privacy Policy appears first at the end of this list; once the apartment is selected, it becomes accessible also in the right band of the website. It is, however, not possible to click on the link, i.e. the Privacy Policy can be read only if the link is copied into a new browser window.

As the last step of reservation, the future guests must provide their personal data and have to tick a box stating that they have read and accepted the terms and conditions of use and the provisions of the Privacy Policy³, but a clickable link pointing to the Privacy Policy is not available here either (screenshots: 27. 11. 2019.), i.e. the Privacy Policy is accessible only from the link placed at the bottom of the page or through the link located in the side band of the website, which cannot be clicked.

³ "I have read and accepted the Terms and conditions and Privacy Policy."

Based on the above, the Authority established that the Obligee infringed Article 12(1) of GDPR as it provides information to the data subject on the processing of their personal data in a form that is not easily accessible.

IV.2. Meeting the Client's access request

The Client submitted a request for the exercise of his right of access to the Obligee on 7 November 2018, which the Obligee answered in merit only on 19 July 2019 after being called upon to do so by the Client on 11 July 2019, and after the notification of the Authority on launching the investigative procedure.

Hence, the Authority establishes that the Obligee infringed Article 12(3) of GDPR with respect to the Client's access request, as it informed the Client on the processing of his personal data only after the one-month period specified in GDPR.

In view of the fact that the Obligee took action to remedy the infringement only after learning of the procedure by the Authority, i.e. the Client did not receive any information on the processing of his personal data for more than seven months from the submission of his access request, the Authority also establishes the infringement of the Client's right to access according to Article 15 of GDPR.

IV.3. The adequacy of the answer given to the Client's access request

The Client requested information on all his personal data processed by the Obligee taking into account all the circumstances of Article 15 of GDPR.

As against this, Obligee only informed the Client that it was processing his personal data in accordance with the Accounting Act. It is the position of the Authority that the Client cannot be expected to know the provisions of the Accounting Act.

In its answer, the Obligee did not tell what personal data were processed for what purpose and for how long, nor was the Client informed on whether or not the Obligee communicated his personal data to third persons. Moreover, it failed to inform the Client on the rights due to him in relation to data processing (GDPR Article 15(1)(e)), or of the fact that he may turn to the supervisory authority with his complaint (GDPR Article 15(1)(f)).

The Privacy Policy attached to the reply provides general information on the processing of data, i.e. it serves to meet the general obligation to provide information according to Article 13 of GDPR. As against this, in the case of requests aimed at exercising the right to access according to Article 15 of GDPR, the information to be provided must be concrete and cover the actual processing implemented in relation to the given data subject, because short of this the data subject's right to check the lawfulness of the processing of his personal data is breached.

Providing information by way of the Privacy Policy is inadequate in the case of an access request, because the Privacy Policy provides information on all data processing, even if it is contingent, and not all of these processing acts are relevant in relation to processing the data of the particular data subject. It is the obligation of the controller to assess how it actually processes the personal data of a given data subject and it is of this that it must provide information based on an access request according to Article 15 of GDPR.

The part of the request, which applies to the uploading of personal data to WhatsApp and the storage of the data there cannot be regarded as a request to exercise the right of access as the photo was made of the

document not of the client, but of his companion. The Client did not discuss this in his request sent to the Obligee, it is revealed only from the complaint lodged with the Berlin Data Protection Authority. It follows that these questions of the Client can only be regarded as requesting general information and not as an access request, as the essence of the right to access is that the data subject should get information on the processing of his personal data and not those of third persons.

Based on the above, the Authority establishes that the Obligee infringed the Client's right to access according to Article 15(1) of GDPR, when despite the Client's express request formulated in the access request, it failed to provide information on all the circumstances specified in Article 15(1) of GDPR in relation to the processing of the personal data.

IV.4. The lawfulness of making a photo of the document of the Client's companion and its uploading to the WhatsApp group

In every case, the processing of personal data is an intervention into the privacy of the data subjects. According recital (3) of GDPR, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. Consequently, controllers must consider in the first place whether achieving their desired purpose requires the processing of the personal data. If the purpose can only be fulfilled by processing the personal data, its process should be developed on the basis of the principle of data minimisation, so that as few personal data should be processed as possible for the shortest possible period.

The Obligee's employee made a copy of the document of the Client's companion in order to see whether the personal data provided upon registration were true.

Based on its statement, the Obligee was fully aware that to check whether the personal data provided by its guests are true, it is enough to have the identification documents presented, and it is not necessary to make copies of the documents of guests and to store them.

Based on the above, the Authority established that the Obligee infringed the principle of data minimisation according to Article 5(1)(c) of GDPR by making a photo of the identification document of the Client's companion with a view to checking the correctness of the data provided upon registration.

The employee of the Obligee did not have any of the legal basis listed in Article 6(1) of GDPR for uploading the photo made of the identification document to the WhatsApp group because the data subject did not grant his consent for that, it was not necessary for performing a contract, no legal regulation required him to do so, nor did he have any legitimate interest in doing so that could override the interests and fundamental rights and freedoms of the data subject. The application of the legal basis according to Article 6(1)(d) and (e) of GDPR is, by definition, excluded.

It follows that the Authority established that the employee of the Obligee provided access to the personal data of the Client's companion to the other employees of the Obligee unlawfully without any legal basis, thereby infringing Article 6(1) of GDPR.

IV.6. Legal consequences

IV.6.1. In its data protection procedure launched ex officio, the Authority established based on Article 58(2)(b) of GDPR that the Obligee infringed Article 5(1)(c), Article 6(1), Article 12(1) and (3), and Article 15(1) of GDPR.

IV.6.2. The Authority orders the Obligee to make his Privacy Policy available on the landing page of his website, as well as in the course of reservation, bearing in mind Section IV.1. of the justification of the decision.

IV.6.3. The Authority orders the Obligee to provide information on the processing of his personal data extending to all aspects of processing to the Client, taking Section IV.3. of the justification of this decision into account.

IV.6.4. The Authority orders the Obligee to refrain from making photo recording of identification documents of its guests, bearing in mind Section IV.1. of the justification of the decision.

IV.6.5. The Authority examined whether imposing a data protection fine against the Obligee was warranted.

In this respect, the Authority considered all the circumstances of the case based on Article 83(2) of GDPR and Section 75/A of the Privacy Act. In view of the circumstances of the case, the Authority established that in the case of the infringement exposed in the course of this procedure, a reprimand is not a proportionate sanction of restraining force, hence it is necessary to impose the fine.

First and foremost, the Authority considered that the infringements by the Obligee qualify as infringements in the higher fine category according to Article 83(5)(b) of GDPR as it involved the infringement of the principles of processing and the violation of the rights of the data subject.

In imposing the fine, the Authority assessed the following circumstances as factors increasing the amount of the fine:

- the difficult access to the Privacy Policy as infringement can be regarded as lasting, as it existed for at least a year. In addition, this affected not only the Complainant, but every natural person who reserved accommodation through the website of the Obligee. According to the statement of the Obligee, 829 reservations were made through the website between 25 May 2018 and March 2020 [GDPR Article 83(2)(a)];
- in the course of the processing under review, the Obligee infringed several provisions of GDPR [GDPR Article 83(2)(a)];
- the Obligee's employee would have prevented the Client and his companion from occupying the accommodation earlier reserved and paid for by them, had the Client's companion not allowed him to make a photo of his identification document, i.e. the Client and his companion would have suffered damage, had they not given permission for the unlawful processing of their data [GDPR Article 83(2)(a)];
- Obligee failed to act sufficiently circumspectly in preparing its answer to the access request of the Client and failed to inform the Client of all the circumstances of processing according to Article 15(1) of GDPR even after learning of the investigative procedure, which was the antecedent of this procedure of the Authority [GDPR Article 83(2)(k)];

In the course of imposing the fine, the Authority assessed the following circumstances as factors reducing the amount of the fine:

- the infringements related to the exercise of the Client's right of access affected him alone and according to the Obligee's statement, other than that of the Client, it did not receive any request for the exercise of rights from data subjects since the entry into force of GDPR [GDPR Article 83(2)(a)];

- it was a circumstance indicative of negligence that human failure caused the non-fulfilment of the Client's access request and making the photo of the identification document of the Client's companion was also a result of an employee's error [GDPR Article 83(2)(b)];
- having learned of its failure, the Obligee attempted to fulfil the Complainant's access request [GDPR Article 83(2)(c)];
- this was the first time that the Obligee infringed the provisions of GDPR, earlier it did not commit relevant infringements, which is a substantial mitigating circumstance, which should be taken into account also based on Section 75/A of the Privacy Act [GDPR Article 83(2)(e)];
- the main activity of the Obligee is the provision of accommodation services made use of largely by tourists. The pandemic caused by the COVID-19 virus caused substantial loss of revenue in the second quarter of 2020 in tourism, thus presumably also at the Obligee [GDPR Article 83(2)(k)].

In addition, the Authority took into account that

- the Obligee met its obligation to cooperate with the Authority [GDPR Article 83(2)(f)];
- the established data protection infringements do not affect the special categories of personal data [GDPR Article 83(2)(g)];
- According to the Obligee's 2018 annual report, its pre-tax profits amounted to HUF 61,149,000, while in the year in question it was HUF 55,456,000. The amount of the data protection fine imposed amounts to 0.49% of the Obligee's pre-tax profits [GDPR Article 83(5)];

In imposing the fine, the Authority did not regard the circumstances according to Article 83(2)(d), (h), (i) and (j) of GDPR as relevant for the concrete case.

The Authority determined the amount of the fine acting within its powers of consideration based on legal regulation.

Based on the above, the Authority decided as presented in the operative part.

V. Miscellaneous issues

The powers of the Authority are set forth in Section 38(2) and (2a) of the Privacy Act, its competence extends to the entire territory of the country.

These decisions are based on Sections 80-81 of the General Administrative Procedures Act and Section 61(1) of the Privacy Act. The decision and the warrant become final upon their communication pursuant to Section 82(1) of the General Administrative Procedures Act. Pursuant to Sections 112 and Section 114(1) of the General Administrative Procedures Act, legal remedy against the decision may be obtained through administrative litigation.

The rules of administrative litigation are specified in Act I of 2017 on the Code of Administrative Litigation (hereinafter: Administrative Litigation Act). Pursuant to Section 13(3)(a)(aa) of the Administrative Litigation Act, a tribunal has competence for the administrative litigation against the decision of the Authority and the Budapest Tribunal has exclusive competence with regard to this litigation. Pursuant to Section 27(1)(b) of the Administrative Litigation Act legal representation is mandatory in administrative litigations under the

competence of a tribunal. Pursuant to Section 39(6) of the Administrative Litigation Act, the submission of a petition has no deferring effect on the administrative act entering into force.

Pursuant to Section 9(1)b) of Act CCXII of 2015 on the General Rules for Electronic Administration and Trust Services to be applied according to Section 29(1) of the Administrative Litigation Act and, in view of this, Section 604 of the Civil Procedures Act, the legal representative of the Client is subject to an obligation to maintain contact electronically.

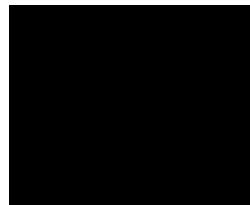
Section 39(1) of the Administrative Litigation Act specifies the date and place of submitting the petition. The information on the possibility of a request for a hearing is based on Section 77(1)-(2) of the Administrative Litigation Act.

Section 45/A(1) of Act XCIII of 1990 on Duties (hereinafter: Duties Act) determines the magnitude of the duty for administrative litigation. Sections 59(1) and 62(1)(h) exempts the party initiating the procedure from the payment of the duty in advance.

Budapest, "16." December 2020



Dr. Attila Petőfalvi
President
Honorary university professor



Summary Final Decision Art 60

Complaint

Administrative fine

EDPBI:HU:OSS:D:2020:167

Background information

Date of final decision:	16 December 2020
Date of broadcast:	17 December 2020
LSA:	HU
CSAs:	DE, DK, ES, FR
Controller:	N/A
Legal Reference:	Lawfulness of the processing (Article 6), Right of access (Article 15)
Decision:	Administrative fine
Key words:	Administrative fine, data minimisation, data subject rights, identity verification, right of access, privacy statement, right to be informed

Summary of the Decision

Origin of the case

The complainant lodged a complaint against the controller with one of the CSAs as a photo was made of his travel companion ID documents and the controller failed to fulfil his request to access to information processed about him.

Findings

The LSA investigated the case and found that the controller infringed a number of provisions of the GDPR. Firstly, Art. 12 GDPR requires controller to provide all information concerning the processing of personal data in a concise, transparent, intelligible and easily accessible form. At the time of the complaint, no page on the website of the controller contained the Privacy Policy. At the time of the decision of the LSA, the Privacy Policy became accessible when the guest began the reservation and chose the date of stay. As the last step of the reservation, guests must tick a box stating that they have read and accepted the terms and conditions of use of the provisions of the Privacy Policy, but a clickable link pointing the Privacy Policy was not available. The LSA found that the controller infringed Art. 12(1) as the information to the data subject was not provided in a form that is easily accessible.

Secondly, the LSA found an infringement of Art. 12(3) GDPR with respect to the access request of the complainant, as the controller informed the complainant after the one-month period specified in the GDPR.

Thirdly, the LSA found an infringement of Art. 15(1) GDPR, as the reply to the access request of the complainant was not adequate in light of this provision.

Lastly, the LSA found an infringement of Art. 5(1)(c) GDPR, as making a photo of the ID documents of the complainant with a view to checking the correctness of the data provided was not found to be in accordance with the data minimisation principle. In addition, uploading this photo on WhatsApp occurred without any legal basis, thereby infringing Art. 6(1) GDPR.

Decision

The LSA found that the controller violated Art. 5(1)(c), Art. 6(1), Art. 12(1) and (3) and Art. 15(1). Firstly, the LSA ordered the controller to make their Privacy Policy available on the landing website and in the course of reservation. Secondly, the LSA required the controller to provide information on the processing extending to all aspects of processing. Thirdly, the LSA ordered the controller to refrain from making photos of ID documents. Taking into account the abovementioned infringements, the LSA imposed a fine of 360,000 forints.



Case no.: NAIH/2020/789/

Official in charge: [REDACTED]

Subject: closure proceedings

The regulatory inspection launched by the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as NAIH) on 28th of November 2018 in relation to the obligations of [REDACTED] (hereinafter referred to as the Controller) under Regulation (EU) 2016/679 ('GDPR') concerning the data breach notified to the NAIH on 16th of November 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 28th of November 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 the NAIH, the following could be established.

The Controller notified the NAIH on 16th of November 2018 that on 2nd of November 2018 it received an e-mail message from an ethical hacker. The e-mail contained information which alluded to the hacking of the Controller's database. Since no other information was available for the Controller it wished to make certain that the hacker's allegations are correct and an unauthorized access to the system had indeed taken place.

Therefore, on 2nd of November 2018 the Controller launched an internal investigation, and commissioned an external expert as well with the execution of a vulnerability test. A blackbox vulnerability inspection was also initiated on 9th of November 2018. As a result, it was determined that the data breach occurred via an SQL Injection through the website [REDACTED] and the fact that an unauthorized access happened [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

The affected databases are related to different operative applications, and the personal data affected are those of employees (e.g. name, e-mail address, username, coded password), athletes applying for sponsorship (e.g. name, height, birth data, weight), Facebook contest winners (e-mail address, name address), persons enquiring via the website (contents of the letter, e-mail address, city, phone number, name) and individuals applying for salesclerk vacancies (name, e-mail address, phone number). The breach may affect 80 individuals, some of whom reside in Member States other than Hungary: Poland – 10 individuals, France – 8 individuals, Spain – 3 individuals, Germany – 2 individuals, Portugal – 1 individual, Denmark - 1 individual.

Judging by the log files the intruder called down only 1-2 data lines from each of the 17 affected data tables, as proof for the detected vulnerability and in hope of a future cooperation with the Controller. He / she neither blackmailed nor threatened the Controller, has not made the data public, and the Controller is not aware of any data transfer having taken place. Considering the circumstances of the case, especially the wording of the letter sent by the hacker to the Controller, the Controller decided that the breach is unlikely to result in a high risk to the rights and freedoms of natural persons, and did not communicate it to the affected individuals.

The controller has internal rules for the handling of data breaches. In this particular case, the IT Department, the data protection officer and the senior management all took part in solving the problem. The attacked system was protected by a firewall, direct access to the databases was possible only from certain IP addresses, and passwords had to be changed every 3 months.

After becoming aware of the data breach, the Controller inactivated the functions that allowed the attack. SQL Injection protection was introduced, and it encompasses all surfaces of the webpage now. No such problem was reported since. Furthermore, the Controller asked the attacker to delete the data gained from the system.

According to Article 32 of the GDPR the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. It is the Controller's task therefore - 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 – to implement the necessary measures in order to provide a secure processing environment.

Based on the circumstances of the case the NAIH concluded that the Controller has not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk, therefore it has not fulfilled its obligation under Article 32 GDPR. This resulted in an unauthorized access the Controller's system and the personal data stored in it. **NAIH issues a reprimand to the Controller**, but, with regard to the facts that

- the hacker has neither blackmailed nor threatened the Controller, has not made the data public (he / she wanted to cooperate with the Controller in the future)
- after having become aware of the breach, the Controller reacted in time and with the right measures
- NAIH agrees with the steps the Controller took to promote the safety of its IT systems and prevent similar future attacks

deems that the reprimand is a sufficient sanction for the breach at hand and sees no reason to open an administrative proceeding 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 January 2021

On behalf of [REDACTED], president of the NAIH:

[REDACTED]
Head of Department

Department of Authorization and Data Breach
Notification



Case number:

Antecedent case number: NAIH/2020/4409.

In charge: [REDACTED]

[REDACTED]

Budapest

[REDACTED]
1075

Honourable [REDACTED],

As you have earlier been informed, the Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information, hereinafter: Authority) received a complaint through the Austrian Data Protection Authority, in which the complainant [REDACTED] (hereinafter: Complainant) submitted that he bought a [REDACTED] at the cash desk of [REDACTED] (registered office: 1075 Budapest, [REDACTED]; hereinafter: Company) located at the [REDACTED] in person on 17 July 2018. In the course of this, the staff member of the Company requested him to provide the number of his identification document because he would not be able to buy the pass without it, therefore the Complainant met the request.

According to the Complainant, the number of his identification document was recorded not only on his pass, but also in the Company's systems; in his view the Company did not have the appropriate legal basis for this and it also infringes the principle of data minimisation. In addition, he also objected to the fact that he did not receive proper information on the processing of the number of his identification document.

Based on 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), an investigation was launched into the case.

I. The course of the procedure

On 8 February 2019, the Austrian Data Protection Authority initiated a procedure to establish the lead and concerned supervisory authorities in accordance with GDPR Article 56 under number A56 ID 59796.

In the procedure according to GDPR Article 56 the Authority indicated on 7 March 2019 that it accepts its designation as lead supervisory authority in this case and at the same time requested the Austrian authority to make the original complaint and all other relevant documents with their English translations available to it, as in the absence of these documents and information it would not be able to conduct the procedure. The Austrian authority failed to respond to this request, though in order to conduct a procedure, the Authority initiated a mandatory mutual assistance procedure in accordance with GDPR Article 61 under No. A61 125465 IMI in the "Internal Market Information System" designed for the exchange of information among data protection supervisory authorities on 14 May 2020. The period open

for responding expired on 14 June 2020, but the Austrian authority did not formally accept the Authority's request.

On 13 August 2020, the Authority uploaded its draft decision to the IMI system, in which it rejected the complaint as obviously unfounded based on the available information.

Following the disclosure of the draft decision on 19 August 2020, the Austrian authority uploaded the documents earlier requested by the Authority in German and in English. At the same time, a staff member of the Austrian authority contacted the Authority by e-mail, informally indicating that they failed to respond to the Authority's request for information because of administrative error, and that they believed that the draft decision was unacceptable as there was no investigation on the merits of the case.

Based on the documents sent, the Authority decided to conduct an investigation on the merits of the case and withdrew its draft decision No. A60 144159 IMI.

In its letter dated 30 September 2020, the Authority informed [REDACTED] that an investigative procedure would be launched in the case and called upon [REDACTED] to make statements in order to clarify the facts of the case. The statement by [REDACTED] was received by the Authority on 19 October 2020.

II. The facts of the case

According to Section I.4 of the Rules of Business, there are two legal relationships that regulate the performance of the passenger transport service used by the passenger. One is covered by the network availability contract, which comes into being between the Company and the passenger, whereby the passenger obtains the right to use the transport network organised by the Company, that is, to travel using the vehicles of the Company or of the contracted service provider partner of the Company, and undertakes the obligation to pay the price of the ticket or pass due to the Company.

The passenger transport service contract comes into being between the passenger and the service provider operating the vehicle, on the basis of which the service provider undertakes to carry the passenger to the destination with its scheduled vehicles.

The pass as a document entitling the holder to travel verifies with respect to the legal relationship according to the valid passenger transport contract and the network availability contract whether the passenger makes use of the services according to the Rules of Business of the Company rightfully. To decide this, the Company has to check the validity of the pass not only with respect to the given period and route network, but it is also indispensable that the Company check whether the valid pass is used by the person entitled to do so. It follows that the pass can only be used – according to the choice of the passenger¹ – together with a pass ID with photo issued by the Company, ID card, passport or driving licence in a card format,² whose number has to be recorded by printing on the pass voucher upon its sale according to Section 3.3 of the Company's tariffs.

When checking the pass, it has to be presented to the person authorised to check together with the pass ID, ID card, passport, etc. According to the Company, failure to record the document identifier on the pass would greatly increase the risk of abuse of non-transferable passes.

The Company informed the Authority that its sales system does not store the identifier numbers given upon the purchase of the pass – it did not do so on 17 July 2018 – in order to enforce the principle of data

¹ Rules of Business Section V.1.2.

² Rules of Business of [REDACTED] (in force: 25 October 2017 - 15 January 2019; hereinafter: Rules of Business) definition according to Section 1.2.

minimisation according to GDPR Article 5(1)(c). It follows that the Company does not process the personal data of the Complainant.

The computer system at the cash desks and the ticket vending machines only print the document identifier to be given upon purchase to the pass voucher; once the printing is done which takes a few seconds only, the document identifier is erased from the temporary memory of the printer. After printing, the data are not recorded in an electronic format or in a data matrix code.

The Company stated that in its view, it does not carry out data processing when printing the document identifiers on the pass vouchers and because of this, it provides information to the passengers on this not in its Privacy Statement but in its Rules of Business. The Rules of Business can be accessed in the website of the Company, in its central customer service, its customer centres and at the cash desks.

III. The findings of the Authority

III.1. Processing carried out by the Company

According to GDPR 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 through availability, alignment or combination, restriction, erasure or destruction.

According to the position of the Authority, distinction has to be made between the two cases when a person buys a pass at the cash desk from a staff member of the Company as the Complainant did, or when he or she buys the pass from a ticket vending machine.

In the first case, the Company staff member while doing his job learns the document identifier either through dictation or by looking at the document used for purchasing the pass, such as a passport, and typing it into the ticket sale system enters it on the pass voucher. In the course of this operation, processing is carried out as the staff member of the Company learns the document identifier as described above either by inspecting it or hearing it as it follows from his job and in relation to it.

When the pass is purchased from a vending machine, it is the passenger himself who types the document identifier on the touch screen of the machine, that is, he does not disclose it to a third person, no third person learns the document identifier.

Irrespective of whether the passenger buys the pass at the cash desk or from the ticket vending machine, in order to display the document identifier on the pass voucher by way of printing, the document identifier has to be stored in the memory of the printer for the period of printing, upon the completion of which the document identifier is erased. During this period, however, the data are stored and it follows that even if for a very short period of time, the Company does carry out data processing.

Beyond this, however, the Company does not collect and does not store document identifiers, it does not process them after printing the pass voucher, thus the further processing of the document identifiers as pseudonym data does not take place as assumed in the Complainant's complaint.

III.2. The lawfulness of processing: necessity

The purpose of indicating a document identifier on the pass voucher is that only one passenger should be able to use the pass voucher, thereby reducing the possibility for abuse.

Document identifiers are unique identifiers, through which a pass voucher and a document with which it is used together can be linked excluding any doubt while the document identifies the passenger who is, the data subject, in other words, the document identifier is the appropriate and relevant data from the viewpoint of the purpose of processing.

According to the position of the Authority, printing the document identifier on the pass voucher – and the data processing carried out for a minimum period of time needed for this, in the given case, learning it by a staff member of the Company and storing it for a few seconds in the memory of the printer – is necessary to prevent abuse and to identify the person entitled to use the pass voucher and it is proportionate to the purpose to be achieved.

The Authority is officially aware that early in the 2010s when there were no ticket vending machines, passengers could buy pre-printed pass vouchers at the cash desks of the Company, and they themselves had to write their document identifiers on them; then the Company did not carry out any kind of data processing. This sales method, however, greatly increased the risk of abuse as many people did not write their document identifiers on the pass voucher, or did so in a manner that could be modified later; thus the pass voucher could be used not only by the person originally entitled to do so, for instance passengers frequently transferred passes no longer used by the passenger buying the pass, but still valid, causing a loss of revenue to the Company.

Based on the above, the Authority establishes that the processing of the document identifier, including the number of the ID card of the Complainant does not infringe the principle of data minimisation as it is a piece of relevant data from the viewpoint of achieving the desired purpose, it is necessary to achieve that purpose and in compliance with the principle of limited storage processing takes place only for the period of time needed to achieve the purpose, that is, until the document identifier is printed on the pass voucher.

III.3. The legal basis of processing

Section 7(4)(a) of Act XLI of 2012 on Passenger Transport Services (hereinafter: Passenger Transport Act) states that the authorisation of the transport service provider providing public passenger transport service extends, *inter alia*, to the identification data of the natural person, such as the surname and given name, surname and given name at birth, place and date of birth, mother's surname and given name at birth, his address, as well as *the type and number of his official certificate suitable for the identification of the person with a view to performing the contract* serving as the basis of the passenger transport service.

The Passenger Transport Act authorises transport service providers providing public passenger transport services, including the Company to process the document identifiers of the passengers entering into contract with it within the framework of performing the passenger transport contract with a view to enabling the checking of the person's right to travel, the identification of the person entitled to travel with a pass voucher and identification during checks.

It is stated in Section 24 of Guideline 2/2019 EDPB that in the context of a contractual relationship there may be a variety of purposes for processing.

According to Section 26 of the Guideline, a controller can rely on Article 6(1)(b) to process personal data when it can establish, in line with its accountability obligations under Article 5(2), both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. According to Sections 27 and 30 of the Guideline, in order to be able to apply GDPR Article 6(1)(b), it is important that the processing of the data be objectively necessary for a purpose that is integral to the delivery of that contractual service to the data subject. The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot as a matter of fact be performed, if the specific processing of the personal data in question does not take place. The important issue here is the nexus between the personal data and the processing operations concerned, and the performance or non-performance of the service provided under the contract.³

According to the position of the Authority, it is objectively necessary for the performance of the contract that the Company be able to identify the other contracting party, i.e. the person who becomes entitled to make use of the Company's services by purchasing the pass in the course of checking the entitlement to travel.

Based on the above, the Authority establishes that the Passenger Transport Act authorises the Company to identify the party contracting by purchasing a pass and to check his entitlement to travel under a passenger transport contract, and pursuant to GDPR Article 6(1)(b) the Company is entitled to process the document identifier from the initiation of the pass purchase by the passenger until the printing of the pass voucher.

III.4. Providing information on processing

Above, the Authority established that although for a very short time, the Company processes the document identifiers of passengers buying non-transferable passes according to their choice. It follows that the Company has an obligation to provide information according to GDPR Articles 13 and 14.

The Company does not dispute that it does not provide information on the processing of the document identifier in the course of printing the pass voucher because in their view, they do not carry out data processing in the course of this.

According to the Authority's position, the Company has an obligation in most cases to provide information according to GDPR Article 13 because characteristically everybody buys the pass for himself or for herself, hence the Company collects the personal data from the data subject; however, there may be cases when somebody buys a pass for a third person, in which case the Company has an obligation to provide information according to GDPR Article 14.

According to GDPR Article 14(5)(a), the controller's obligation to provide information does not exist, if the data subject already has the information. According to the Authority's position, if a third person buys a pass for a data subject, the data subject is doubtless aware that he made his document identifier available to the third person for the purpose of buying a pass [GDPR article 14(1)(d) – categories of personal data

³ The Authority is aware that the Guideline applies to contracts entered into for online services; however, according to the Authority's position, the points thereof also apply in this case in connection with the "objectively necessary" condition required for the performance of the service.

concerned in processing], and the source of the personal data is also known to him [GDPR Article 14(2)(f)].

It follows that the Company is not subject to an obligation to provide information on the above two circumstances based on GDPR Article 14(5)(a) to the data subjects for whom another person buys a non-transferable pass, whose data are given to be processed by the Company not by them.

In such cases, the Company would not be able to provide information of merit, i.e. relevant about the source of the data, or in the given case, the Company is not even aware that the source of the document identifier was not the data subject himself, for instance when a third person buys the pass for the data subject from a ticket vending machine.

Based on this, the additional circumstances of data processing, on which the Company has to provide information pursuant to GDPR Articles 13 and 14 are the same in the two articles, thus it will suffice for the Company to draft a single item of information indicating exactly what data can be provided – such as the number of the pass certificate, ID card, passport – irrespective of the fact that Article 13 does not stipulate this as a requirement, and it would not be mandatory pursuant to Article 14(5)(a).

The Company indeed has a Privacy Statement, thus according to the Authority's position, it may suffice merely to supplement it with the investigated processing, in the course of which the following are relevant among the of the circumstances listed in GDPR Articles 13 and 14, i.e. the Company has to provide information about these over and above the information it already provides: the purpose of the planned processing of personal data, the legal basis of processing, the period of storing the personal data and whether the provision of personal data is based on legal regulation or contractual obligation, whether it is a precondition to entering into contract and whether the data subject is under an obligation to provide the personal data, and furthermore, what are the possible consequences of not providing the data. [GDPR Article 13(1)(c), (2)(a) and (e)].

The Authority finds it necessary not to note that the purpose of processing can be inferred from the Company's Rules of Business, but according to the Authority's position to ensure transparency, it is necessary to inform the passengers of the above circumstances of the investigated processing in the Company's Privacy Statement.

Based on the above, the Authority establishes that the Company failed to meet its obligation to provide information according to GDPR Articles 13 and 14 when it failed to provide information on the fact of processing – in view of the fact that in its view it does not perform data processing – and of the circumstances of processing listed by the Authority above.

III.5. Legal consequences

III.5.1. Based on GDPR Article 58(2)(b), the Authority reprimands the Company because it infringed its obligation to provide information in accordance with GDPR Articles 13 and 14 when it failed to provide information on the fact of processing the document identifiers and the circumstances of processing indicated in Section III.4.

III.5.2. Pursuant to GDPR Article 58(2)(d) and Section 56(1) of the Privacy Act, the Authority calls upon the Company to provide information to the data subject on the fact of processing and its circumstances according to GDPR Article 13(1)(c), 2(a) and (e) by supplementing its Privacy Statement, or if it so chooses in a separate Privacy Statement.

The Authority informs the Company that pursuant to Section 56(2) of the Privacy Act, the Company has to take the necessary measures indicated in this call if it agrees with them, and has to inform the Authority of the measures taken and the evidence thereof, or if it disagrees of its position in writing within thirty days from receipt of this call.

Pursuant to Section 58(1)-(2) of the Privacy Act, if the infringement is not remedied as a result of this investigation and the direct threat of infringement is not terminated, the Authority will decide on taking any necessary additional measures within thirty days following the expiry of the thirty-day period open to provide information.

Budapest, " " 2021

Yours sincerely,

Dr. Attila Péterfalvi
President
Honorary university professor

Delivery clause to file number NAIH/**To:**

	Name, mailing address of the addressee:	To be attached	Mode of mailing
1.	To [REDACTED] <u>Budapest</u> [REDACTED] 1075	-	registered letter with acknowledgement of receipt
2.	[REDACTED]	-	e-mail
3.	Archives	-	-



Case no.:NAIH-...../2021.
NAIH/2020/3232.

Hamburg Commissioner for Data Protection and Freedom of Information
(Der Hamburgische Beauftragte für Datenschutz- und Informationsfreiheit)

To be delivered via IMI-System

Budapest, July ____, 2021

To Whom It May Concern,

A complaint has been lodged with the Data Protection Authority of Hamburg, in which an anonymous complainant objected to the data processing of [REDACTED] Ltd. (hereinafter referred to as Ltd.). According to the complaint, the Ltd. disclosed the e-mail address of the complainant on the website of [REDACTED] (hereinafter referred to as website), which resulted for the complainant to receive a large number of unsolicited e-mails. Furthermore, according to the complaint, the source code of the website contained e-mail addresses relating to numerous other companies, and the complainant presumed that the consents of the mentioned companies were missing as well. The complainant further stated that the Ltd. operated other similar websites (the complaint lacked more precise information) on which numerous e-mail addresses appeared.

In the procedure set out in Article 56 of the general data protection regulation (GDPR)¹ for the designation of lead and concerned supervisory authorities, under the number of IMI-114383 the Data Protection Authority of Hamburg designated the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter referred to as "the Hungarian Authority") to be the lead authority. In this procedure the Hungarian Authority agreed thereto, as according to the publicly available domain registry, the registered user of the website on April 1, 2020 was the Ltd. As according to the Hungarian official company register the Ltd. was indeed a commercial business entity registered under the seat of [REDACTED], [REDACTED], and having regard to the registered seat (probably the main place of operation) the Hungarian Authority's presumption was that it shall act as lead Authority in accordance with Article 56. 1 of the GDPR.

Thereafter, the Hungarian Authority commenced an investigation pursuant to Article 57. 1. (f) of the GDPR and Section 38. 3 (a) of the Act CXII of 2011 on the right to informational self-determination and on the freedom of information (hereinafter "the Act CXII of 2011").

During the investigation, the Authority viewed the website several times and saved the webpages (for the first time on April 1, 2020), the website advised its visitors that it was in under maintenance operation, however, simultaneously several e-mail addresses appeared on the website, and some of those probably were of real natural persons. In addition thereto, the website provided the information that these e-mail addresses were spam traps to spam bots (sending unsolicited advertising messages or placing unsolicited advertisements), and warned the visitors as follows:

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)

(„These are spam traps to spam bots. Do not send any e-mails to them otherwise your address will be added to spam lists.”)

On May 13, 2020 the Authority contacted the Data Protection Authority of Hamburg in a mutual assistance procedure referred to in Article 61 with a request registered under the case no. of IMI-125264 to upload the complaint to the IMI-system, and, if available, the English translation thereof. The reason of the request – which the Hungarian Authority also communicated – was to clarify whether the subject of the complaint was the data processing of the Ltd. in general or only with regard to complainant's own case. By referring to the fact that the website was under maintenance operation, as mentioned above, the Hungarian Authority required the statement of the complainant as to whether the complainant would maintain or, under a certain circumstance, withdraw his/her complaint (as it could not be established as to in which timeframe was the content objected). The deadline for complying with the request of the Hungarian Authority was June 13, 2020, however, as the Authority of Hamburg did not react to this request, the Hungarian Authority sent a reminder on June 26, 2020 via e-mail to the address of [REDACTED]. The Hamburg Authority on July 16, 2020 informed the Hungarian Authority via the case register opened under the registration no. of IMI-138412 that the Complainant did not wish to have his/her personal data forwarded to Hungary (to the Hungarian Authority), and that the concerned Authority of Hamburg was not in a position to decide whether the complainant is a directly concerned data subject, as the complainant's e-mail address did not appear among the e-mail addresses in the source code of the website. However, as the source code contained more than 2900 .de extension e-mail addresses, and some of those contained personal data as well (<first name>.<family name>@domain.de), the opinion of the Authority of Hamburg was that such addresses needed to be eliminated from the website as soon as possible. The Authority of Hamburg did not know as to what purpose could the display of several thousand e-mail address serve.

Thereafter, the Hungarian Authority in order to assemble the bearings of the case sent an inquiry to the Ltd. in which it asked

1. the Ltd. to present its operation in connection with the [REDACTED] website;
2. whether the Ltd. had previously determined or at that time determined the content, the contact details, and the personal data on the website, in particular the e-mail addresses, or had previously defined or at that time defined the purposes of the processing of personal data appearing thereon, in other words, could the Ltd. be identified as data controller in connection with the website. If the answer was to be negative, the Hungarian Authority requested the Ltd. to provide information on the identity of the data controller person/entity and the postal or electronic contact detail thereof;
3. as to what were the sources of the personal data accessible on the website; what were the legal basis of the data processing pursuant to Article 6.1 of the GDPR; what was the purpose of the data processing; and what was the time period of the processing of these personal data;
4. as to how had previously or at that time informed the Ltd. the data subjects using the e-mail addresses accessible on the website of their rights in compliance with Article 12-14 of the GDPR;
5. as to how had previously ensured or at the time ensured the Ltd. the data subjects' rights according to GDPR Chapter III in connection with the personal data accessible on the website.

Apart from those above, the Hungarian Authority requested the Ltd. to inform the Hungarian Authority of any fact or circumstance which might have merit in the case.

The answer of the Ltd. arrived on September 8, 2020 to the Hungarian Authority and it answered to the questions in their posed order as follows:

1. The Ltd. had no knowledge of the mentioned domain, the domain had never been under its control. According to the statement of the Ltd., it had not registered by the given domain service provider, but later, during the communication with the Authority, it did, and based on the experience of the Ltd., there were not any control regarding the identity of the domain registrant. As per the statement of the Ltd., its affiliate partners also had not registered the website on behalf of the Ltd.
- 2-5. The Ltd. did not know of the content of the website, it did not process the e-mail addresses forwarded by the Hungarian Authority (the Authority attached to its inquiry the content available at the time of the inquiry).

Thereafter, the Hungarian Authority revisited the website, and as per its state on December 1, 2020, the previous content which was accessible during the procedure carried out pursuant to Article 56. of the GDPR had been eliminated (saved pages thereof attached); according to the data available on December 1, 2020 of the publicly accessible domain registry, the user of the website was a natural person, [REDACTED], located in [REDACTED] another town in Hungary, who, according to the Hungarian official company register, was neither a member nor an executive officer of the Ltd.

Based on the information available to the Hungarian Authority, the data controller could not be identified, therefore, the Authority's opinion is that the competence of the Hungarian Authority to act as lead supervisory authority cannot be established pursuant to Article 56.1 of the GDPR. As the efforts of the Hungarian Authority to identify the data controller were of no avail, and as it cannot carry out further investigation, and additionally, as the objected content is no longer available, the Authority closes the case.

Sincerely,

Attila Péterfalvi, PhD.
President
Honorary Professor

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 19th day of May 2023



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 7 July 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 of the GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) of the GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 17 April 2022 to request the erasure of their account on the Respondent’s Instagram platform, to which they no longer had access.
 - b. The Data Subject did not receive any response from the Respondent and therefore lodged a complaint directly with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that

- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 18 January 2023, the Respondent advised the DPC that it had contacted the Data Subject directly. As part of this contact, the Respondent advised the DPC that it had assisted the Data Subject in regaining access to their account and as such, the Data Subject was able to make use of the self-serve deletion tool in order to schedule the permanent deletion of their account.

8. On foot of the response provided by the Respondent, on 20 January 2023 the DPC contacted the Data Subject to confirm whether or not the action taken by the Respondent satisfactorily resolved their complaint.

9. On 20 February 2023, the Data Subject confirmed to the DPC that they were successful in obtaining access to their account and thanked the DPC for its assistance. The Data Subject also noted that they had successfully scheduled their account for erasure.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;

 - b. The agreed resolution is such that the object of the complaint no longer exists; and

 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Dutch Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Dutch Data Protection Authority (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 4 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request directly to the Respondent on 5 June 2020.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

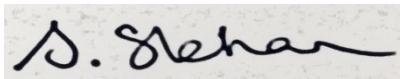
7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject's account was suspended by the Respondent due to a purported serious violation of its Service Agreement. In the circumstances, the Respondent agreed to take the following action:
 - a. Provide the DPC with the specific reasons for the Data Subject's account suspension and provide an explanation as to why their account must remain suspended.
8. The DPC subsequently wrote to the Data Subject via the Recipient SA, explaining that their account was suspended for a purported serious violation of the Respondent's Service Agreement and that, based on the information provided by the Respondent, it was entitled to rely on Article 15(4) GDPR to refuse providing them with their requested data, on the basis that it would adversely impact the rights and freedoms of others.
9. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and

- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "S. Skehan".

Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bavarian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 21 December 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Bavarian Data Protection Authority (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 11 March 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. On 17 November 2020, the Data Subject submitted an access request to the Respondent, seeking access to their personal data.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

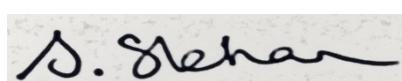
Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject's account had been suspended due to a violation of the Respondent's Service Agreement. In the circumstances, the Respondent took the following action:
 - a. The Respondent agreed to share the specific reasons for the Data Subject's account suspension with the DPC, on a confidential basis.
- 8. On 31 May 2021, the DPC outlined the complaint to the Respondent, noting that they sought a copy of all their personal data. On 19 August 2021, the Respondent confirmed to the DPC that the Data Subject's account was suspended for a violation of its Services Agreement, and provided the DPC with the specific reasons for the Data Subject's account suspension on a confidential basis. The Respondent confirmed that its customer support team had reviewed the Data Subject's appeals of its decision to suspend their account, but that the suspension had been upheld.
- 9. On 8 September 2021, the DPC contacted the Data Subject via the Recipient SA. The DPC informed the Data Subject that it had sought clarification from the Respondent in relation to the Data Subject's account suspension, including information on the investigation carried out, the decision-making process which led to the Data Subject's account suspension, and whether the Data Subject had exercised any appeal mechanism. The DPC informed the Data Subject that it had reviewed the reasons for their account suspension provided by the Respondent and that it was satisfied that it had complied with its obligations under Article 15 GDPR. The DPC noted that it was now clear that the remaining aspects of the complaint related solely to the manner in which the Respondent had enforced its terms and policies, an issue not falling with the scope of the GDPR or the 2018 Act. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.
12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Bavarian Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 21st day of October 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 20 June 2018, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Bavarian Data Protection Authority (“the **Recipient SA**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 17 June 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request pursuant to Article 15 GDPR to the Respondent on 15 June 2018. On 19 June 2018, the Respondent responded to the Data Subject explaining how they could access their requested data by logging into their Microsoft account.
 - b. The Data Subject was not satisfied with the Respondent’s response, as they wished to access all data held in relation to them, not limited to the data connected to their Microsoft account.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent was willing to conduct a search for any personal data relating to the Data Subject outside of their Microsoft account, but it required the Data Subject to initiate the request themselves for security and privacy reasons. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent outlined that in order to facilitate the Data Subject’s access to data processed about them outside of their Microsoft account, the Data Subject was first required to initiate such a request themselves for security and privacy reasons.
 - b. Subsequently, the Data Subject would be required to authenticate their request by providing and validating ownership of ‘alternate identifiers’ such as email address, phone number and/or postal address before the Respondent could perform an internal search for the data requested.
8. On 18 November 2020, the DPC outlined to the Data Subject the prerequisites to be met in order for the Respondent to facilitate access to the personal data processed outside of their Microsoft account. On 22 November 2020, the Data Subject responded to the DPC stating that they were not satisfied with the Respondent’s response. The Data Subject asserted that Microsoft’s procedures, in particularly its authentication procedure, were too complicated. The Data Subject also objected to having to potentially disclose further personal information to the Respondent.
9. Following further engagement by the DPC, the Respondent subsequently outlined in more detail the security reasons behind its requirement for additional authentication before facilitating access to data not directly associated with a Microsoft account. The Respondent noted that for data which is associated with a Microsoft account it has remote secure systems, including in-app tools, which enable data subjects to access and control their personal data.

However, for personal data not directly associated with a Microsoft account, the Respondent stated that requests for this data can be made via its online request form. The Respondent noted that, for these types of requests being made, which are not directly linked to a Microsoft account, it requires the data subject to authenticate their request by providing and validating ownership of a number of identifiers, including their email address and phone number. The Respondent noted that these measures are in place to protect the privacy and security of all of its users against social and technical manipulations that attempt to phish or otherwise compromise users, and to prevent the unintentional exposure of personal data to unauthorised third parties. Separately, the Respondent provided the DPC with a copy of correspondence it had issued to the Data Subject directly, explaining how they could authenticate their request, and explaining why it required this additional authentication. On 10 August 2021, the DPC wrote to the Data Subject outlining the Respondent's response, including why the Respondent required the Data Subject to authenticate their request before providing them with the requested data. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

10. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018, is deemed to have been withdrawn by the Data Subject.

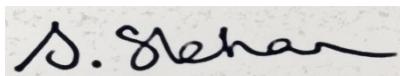
Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022, the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Sandra Skehan
Deputy Commissioner

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 September 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent and requested the delisting of several URLs from its search engine.
 - b. The Data Subject was not satisfied with the Respondent’s response to their delisting request.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject had provided additional relevant information to the DPC when making their complaint, which had not previously been provided to the Respondent. In the circumstances, the Respondent agreed to take the following action:
 - a. The Respondent agreed to reassess the Data Subject's delisting request; and
 - b. Following this reassessment, the Respondent agreed to delist the requested URLs.
- 8. On 12 November 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC provided the Respondent with the list of URLs that the Data Subject requested to be delisted. These URLs related to legal proceedings before the Irish Labour Court, in which the Data Subject had been involved.
- 9. On 29 November 2021, the Respondent informed the DPC that the Data Subject had provided the DPC with additional relevant information that was not provided to the Respondent at the time of the Data Subject's original delisting request; namely, that there had been a decision by the Labour Court to remove its determination in the Data Subject's case from its website.
- 10. On 31 January 2022, the DPC requested documentation from the Data Subject confirming that the information relating to their case should be treated as private information, per the decision of the Labour Court. The Data Subject provided the DPC with the requested documentation on the same date. The DPC subsequently forwarded this confirmation to the Respondent, asking it to consider this information in relation to the Data Subject's delisting request. On 5 April 2022, the Respondent confirmed that the requested URLs had been delisted. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
- 11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 11 January 2022, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting access to their personal data, followed by the subsequent erasure of their personal data. The Data Subject's requests were made following the suspension of their Hinge account.
 - b. The Data Subject asserted that they did not receive any response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that at the time of receiving the DPC's correspondence, the Data Subject's appeal was in a queue for review by the Respondent's Trust & Safety team. In the circumstances, the Respondent took the following action:
 - a. The Respondent reviewed the Data Subject's appeal of their account suspension and decided to lift same from the Data Subject's account. The Respondent agreed to grant the Data Subject with immediate access to their requested personal data and wrote directly to the Data Subject confirming same; and
 - b. The Respondent provided the Data Subject with the instructions on how they could download and access their requested data.
8. On 6 May 2022, the DPC outlined the Data Subject's complaint to the Respondent. The DPC informed the Respondent that the Data Subject stated that they had appealed their account suspension, but that they did not receive a response from the Respondent. The DPC stated that the Data Subject requested access to all of their personal data, including photos that had been uploaded to their account, followed by the erasure of all of their data. The DPC raised a number of queries with the Respondent in relation to its investigatory steps leading to the Data Subject's account suspension, and the decision-making process, which led to the suspension of their account, including confirmation as to whether or not any appeal mechanism was exercised by the Data Subject.
9. On 20 May 2022, the Respondent responded to the DPC. The Respondent provided the DPC with a response addressing the DPC's queries, which was forwarded to the Data Subject with the Respondent's permission. The Respondent confirmed that the Data Subject's account suspension had been lifted, and that they now had access to their account, and could make use of its self-service tools to download their data and close their account, if they so wished. The Respondent explained to the DPC that its automated tools had flagged the Data Subject's account for review after detecting behaviour that potentially violated its terms and conditions. The Data Subject's account was subsequently reviewed and it was determined that it had appeared to violate its terms and conditions. The Respondent informed the Data Subject of the account suspension on 13 December 2021. The Respondent also confirmed to the DPC

that the Data Subject had appealed its decision, and that the Respondent had been in regular contact with the Data Subject regarding their appeal. The Respondent informed the DPC that, at the time of receiving the DPC's correspondence, the Data Subject's appeal was in a queue for review by its 'Trust & Safety team'.

10. On 8 June 2022, the DPC wrote to the Data Subject, outlining the Respondent's response. When doing so, the DPC noted that the Respondent had now reviewed the Data Subject's appeal and lifted their account suspension. As such, the Data Subject could now use the Respondent's self-service tools to download a copy of their data, and that they could now close their account if they wished. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to be amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 4th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 December 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 28 December 2021 seeking the full erasure of their personal data from the Respondent's platform under Article 17 GDPR.
 - b. In response to this request, the Respondent directed the Data Subject to the platform's in-app tool. The Respondent advised the Data Subject that by using this in-app tool, they could begin the deletion process of their personal data.
 - c. The Data Subject was not satisfied with the response received from the Respondent, as they had reservations as to whether this process would be sufficient to obtain the full erasure of their data. On this basis, the Data Subject made a complaint to the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, on 22 June 2022, the Respondent confirmed to the DPC that the Data Subject had already utilised the in-app tool and deleted their account, which resulted in the erasure of their personal data. The Respondent further confirmed that this action occurred prior to the DPC commencing the complaint with the Respondent.
8. Following receipt of this correspondence from the Respondent, the DPC wrote to the Data Subject on 06 July 2022, confirming that their data had now been deleted. In the circumstances, the DPC asked the Data Subject to notify it, within the specified timeframe, if they were not satisfied with the outcome, so that the DPC could consider the matter further.
9. The DPC can confirm that no response has been received from the Data Subject in relation to this.
10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink that reads "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 11th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 4 August 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 28 April 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s account was suspended by the Respondent. The Data Subject subsequently submitted an erasure request to the Respondent under Article 17 GDPR on 30 June 2020. As part of this request, the Data Subject specifically requested to have their phone number erased from the platform.
 - b. The Respondent replied to the Data Subject by email on the same date, noting that certain personal data would be retained in line with the Respondent’s privacy policy. The Data Subject was dissatisfied with the response received from the Respondent and believed that the Respondent had not fulfilled their request for erasure.
 - c. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with their supervisory authority

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account and following this suspension, it had retained the Data Subject’s personal data. According to the Respondent, the retention of this data was in line with the Respondent’s data retention policy. Following engagement between the Respondent and the DPC, the Respondent agreed to take the following action:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s suspension. Following this review, the Respondent chose to lift the suspension. By lifting the suspension, this action provided the Data Subject with access to their account and the ability to self-delete the account, should they still wish to do so.
 - b. The Respondent communicated the outcome of their review to the Data Subject on 01 June 2022, and informed the DPC of this on the same date.
- 8. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Data Subject on 28 June 2022 via the Recipient SA. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 29 August 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
- 9. On 16 September 2022 and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Spanish Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

**Further to the requirements of Internal EDPB Document 06/2021 on the practical implementation
of amicable settlements (adopted on 18 November 2021)**

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF INTERNAL EDPB DOCUMENT 06/2021 ON
THE PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS, ADOPTED 18 NOVEMBER 2021**

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 23 May 2020, [REDACTED] (“the Data Subject”) lodged a complaint pursuant to Article 77 GDPR with the Spanish Data Protection Authority (“the Recipient SA”) concerning Microsoft Ireland Operations Limited (“the Respondent”).
2. In circumstances where the Data Protection Commission (“the DPC”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 28 October 2020.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted a delisting request to the Respondent in respect of a number of URLs.
 - b. The Data Subject was not satisfied with the Respondent’s response.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the 2018 Act”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the Respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise his/her data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 (“Document 06/2021”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent had initially declined to delist the requested URLs but that, following further engagement with the DPC, it would now delist the URLs. In the circumstances, the Respondent took the following action:
 - a. The Respondent delisted the requested URLs.
- 8. On 1 February 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that the Data Subject considered that the contents of the URLs were inaccurate. The DPC also outlined that the Data Subject believed that the URLs were having a negative impact on both their private and professional life. On 15 February 2021, the Respondent informed the DPC that, at the time of its initial rejection of the Data Subject's delisting request, it had concluded that the Data Subject was currently involved in active litigation. As such, the Respondent had refused the delisting of the URLs as the information was of public relevance. However, the Respondent stated that it would be willing to re-evaluate its position and delist the requested URLs if the litigation which the Data Subject was involved in was now concluded, and if they submitted a new delisting request. The DPC subsequently wrote to the Recipient SA, outlining the response of the Respondent.
- 9. The DPC subsequently received correspondence from the Recipient SA on 24 April 2021, stating that, in its view, the Data Subject had already made a valid delisting request, and the Respondent should not require them to submit another request. Furthermore, the Recipient SA could not find any evidence online of the Data Subject being involved in active litigation, nor did the Data Subject inform it at the time of their complaint that they were involved in any litigation. Following further engagement with the Respondent, on 21 July 2021 the DPC received confirmation from it that the complained-of URLs were no longer returning against a search of the Data Subject's name on Bing Spain.
- 10. On 8 September 2021, the DPC wrote to the Respondent, pointing out that the complained-of URLs were still returning in a Bing search conducted by the DPC, and that the relevant case law on the "right to be forgotten" had concluded that search engine operators are required to remove all the links on all versions of its search engine in the EU, regardless of where the request to delist originates in the EU. Following further engagement with the Respondent, it confirmed to the DPC on 23 September 2021 that it was in the process of delisting the

complained-of URLs. On 4 October 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the latest response received from the Respondent. The Recipient SA sent the DPC's letter to the Data Subject on 14 October 2021. In the circumstances, the DPC asked the Data Subject to notify it, within two months if he/she was not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2021, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 27 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent by post on 25 March 2021, requesting access to their personal data. The Data Subject also noted that a previous access request submitted to the Respondent on 4 February 2021 was not completed.
 - b. The Data Subject wrote to the Respondent again on 27 April 2021, outlining that neither of their two previous access requests had been completed. The Data Subject asserted that they did not receive a response from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps, as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the email address the Data Subject had contacted was not a valid email address for the Respondent, however, the access request they had made by post had not been responded to. In the circumstances, the Respondent took the following action:
 - a. The Respondent explained to the DPC that due to an administrative error, the access request made by post was not forwarded to the appropriate team. The Respondent confirmed that it has since rectified this issue;
 - b. The Respondent wrote directly to the Data Subject, providing them with data download links to access their personal data.
8. On 17 September 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that it had already established with the Respondent that the email address used by the Data Subject to make their access request of 4 February 2021 was not a valid email address for the Respondent, and had informed the Data Subject of same. The DPC requested that the Respondent respond to the substance of the Data Subject's access request and provide the Data Subject with information about the processing of their personal data.
9. On 5 October 2021 and 13 October 2021, the DPC received correspondence from the Respondent, confirming that it had written to the Data Subject directly in response to their access request and had provided the Data Subject with information regarding the processing of their personal data. The Respondent also explained that due to an administrative error, the Data Subject's access request made by post was not forwarded to the appropriate team at the time. The Respondent confirmed that that this internal issue has since been rectified, and that it had apologised to the Data Subject for the delay in responding to their access request.
10. On 26 October 2021, the DPC engaged further with the Respondent, highlighting that the Data Subject had stated in their original correspondence that they did not wish to use the Respondent's tools to exercise their rights under the GDPR and was not legally required to do so. The DPC highlighted that the Data Subject wished to receive their data by email.

11. On 1 November 2021, the Respondent confirmed to the DPC that it had written to the Data Subject again, providing a data download link in respect of each of their accounts. On 9 November 2021, the DPC outlined the Respondent's correspondence to the Data Subject. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to be amicably resolved.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 25 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - The Data Subject emailed the Respondent on 26 April 2019, to request the deletion of their Facebook account and personal data under Article 17 GDPR. The Data Subject received a response from the Respondent on the same day that the account would be scheduled for deletion on 26 May 2019. However, the Data Subject continued to receive correspondence from the Respondent after this date had passed.
 - As a result of this, the Data Subject thereafter lodged an access request, under Article 15 GDPR, to ascertain what personal data was held about them by the Respondent. This request was lodged on 12 May 2021, and the Data Subject was advised on the same day that no account pertaining to the Data Subject remained on the Respondent’s platform.
 - The Data Subject was dissatisfied with the response received from the Respondent, and believed that the Respondent had not fulfilled their requests. On this basis, the Data Subject lodged a complaint with their local supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
- the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that no account pertaining to the Data Subject existed on the Respondent’s platform. However, the Respondent confirmed that the Data Subject had previously subscribed to marketing emails from a “*Metafor Developers*” mailing list. The Respondent advised that subscription to this mailing list, and the receipt of related marketing emails, were unconnected to the existence of a Facebook account, thus explaining why the Data Subject continued to receive correspondence from the Respondent. In the circumstances, the Respondent agreed to take the following action:
- The Respondent agreed to ensure that the Data Subject was fully opted-out from receiving such marketing emails, which would prevent them from receiving such emails or similar notifications in the future.
8. The DPC’s letter outlining the actions taken by the Respondent as part of the amicable resolution process issued to the Recipient SA on 03 May 2022, for onward transmission to the Data Subject. This letter issued to the Data Subject on 24 May 2022. In its correspondence to the Data Subject, the DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the actions taken by the Respondent, so that the DPC could take further action. On 08 September 2022, the Recipient SA confirmed that no response had been received from the Data Subject.

9. On 20 September 2022 and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

10. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

11. For the purpose of Document 06/2022, the DPC confirms that:

- The complaint, in its entirety, has been amicably resolved between the parties concerned;
- The agreed resolution is such that the object of the complaint no longer exists; and
- Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

12. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 25th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 18 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited) (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent via a posted letter on 29 February 2020, requesting the erasure of their Facebook account and all associated personal data. The Data Subject also provided the Respondent with four email addresses and requested the erasure of any Facebook accounts associated with these email addresses.
 - b. The Data Subject noted that as they received no response to this initial letter, they again contacted the Respondent via a posted letter on 29 July 2021, requesting the erasure of the aforementioned personal data under Article 17 GDPR.
 - c. The Data Subject confirmed to the DPC on 30 October 2021 that they had still not received any response from the Respondent to their request, and as such wished to pursue this matter further with the DPC.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
- 6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent confirmed to the DPC, on 16 May 2022, that it could only identify one account that remained on the platform and that appeared to be associated with the Data Subject. However, the Respondent acknowledged that the Data Subject could no longer access this account. In the circumstances, the Respondent agreed to take the following action:
 - a. If the Data Subject supplied the Respondent with a new secure email address, then the Respondent would engage directly with the Data Subject to assist them in regaining access to the account. By regaining access to the account, the Data Subject could then initiate the self-deletion of their account.
- 8. On 09 June 2022, the DPC wrote to the Data Subject, informing them of the Respondent’s offer to help them regain access to their account, should they provide a new secure email address. On 24 June 2022, the Data Subject responded to the DPC, noting that they agreed to this offer of amicable resolution, and supplied a new secure email address that could be passed on to the Respondent.
- 9. Having provided the Respondent with the requested information, the Respondent confirmed to the DPC that its specialist team had reached out to the Data Subject, on 18 July 2022 and 24 July 2022, to verify account ownership and assist them in regaining access to the relevant Facebook account.

10. Following receipt of this confirmation from the Respondent, the DPC wrote to the Data Subject on 11 August 2022. This letter requested a response from the Data Subject within two months if they objected to the amicable resolution of their complaint and wished to pursue the matter further.
11. The DPC can confirm that the Data Subject responded to the DPC acknowledging receipt of this letter.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburg Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 24th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Hamburg Data Protection Authority ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 15 February 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent requesting a copy of their personal data and information in relation to all the categories of personal data referred to in Article 15(1)(a)-(h) of the GDPR.
 - b. The Data Subject stated that they did not receive a reply to their access request from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent was unable to locate an active account associated with the email address provided by the Data Subject. The Respondent noted that the Data Subject previously had a Facebook account, but that it appeared that they had self-deleted their account. In the circumstances, the Respondent took the following actions:
 - a. The Respondent confirmed to the DPC that it had conducted an internal investigation in relation to the Data Subject’s access request and determined that there wasn’t a Facebook account associated with the email address provided by the Data Subject; and
 - b. The Respondent provided a link for the Data Subject’s attention, containing information about what happens to permanently deleted accounts from its platform.
8. On 31 March 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted that the Respondent had previously confirmed to the Data Subject that their request had been forwarded to its relevant support team, but that the Data Subject maintained that their access request had not been fulfilled.
9. On 28 June 2021, the Respondent responded to the DPC. The Respondent informed the DPC that it had conducted an internal investigation and could not find any account linked to the email address provided by the Data Subject. The Respondent stated that it appeared that the Data Subject had self-deleted their account and therefore it no longer processed data in relation to them. As such, it could not provide a further response to the Data Subject’s access request.
10. On 12 August 2021, the DPC wrote to the Data Subject via the Recipient SA, outlining the information provided by the Respondent. The DPC provided the Data Subject with a link to an information page supplied by the Respondent, which contained information on what happens when a Facebook account is permanently deleted from the Respondent’s platform. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were

not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 1 November 2021, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburg Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited.

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 24th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 2 March 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Hamburg Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 5 May 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 21 February 2020, requesting information about how the Respondent processes their personal data, and seeking access to any personal data specifically related to their use of the Respondent’s facial recognition technology.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps, as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent did not hold any facial recognition data in relation to the Data Subject. In the circumstances, the Respondent took the following actions:
 - a. The Respondent confirmed to the DPC that it does not hold any facial recognition data relating to the Data Subject; and
 - b. The Respondent provided the DPC with a copy of correspondence it had sent to the Data Subject directly on 20 August 2021, addressing their access request and confirming that it does not hold facial recognition data in relation to him.
8. On 28 July 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC requested that the Respondent write to the Data Subject responding to the substance of their access request and, in particular, address their concerns in relation to their facial recognition data.
9. On 20 August 2021, the Respondent responded to the DPC. The Respondent confirmed to the DPC that it had contacted the Data Subject directly regarding their request for access to their facial recognition data, and that it does not hold any facial recognition data in relation to them, as they have turned off the facial recognition setting on their account. The Respondent subsequently provided the DPC with a copy of correspondence sent to the Data Subject, in which it confirmed that it does not hold facial recognition data in relation to them, and providing further information on how its facial recognition technology operates.
10. On 24 September 2021, the DPC contacted the Data Subject via the Recipient SA. When doing so, the DPC noted that the Respondent had contacted the Data Subject directly and addressed their concerns in relation to their facial recognition data. The DPC informed the Data Subject that the Respondent had also stated that it had substantively addressed the balance of their original access request in its correspondence with them of 25 February 2020, including providing step-by-step instructions on how to access and download their data using its in house tools. In the circumstances, the DPC asked the Data Subject to notify it, within two

months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

11. On 3 December 2021, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 18th day of November 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 October 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority ("the **Recipient SA**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. In circumstances where the Data Protection Commission ("the **DPC**") was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 16 November 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request directly to the Respondent on 3 July 2021, requesting a copy of their personal data.
 - b. The Data Subject asserted that they could no longer access their personal data through the Respondent's self-service tools, as they were being redirected to an identity verification window upon login. The Data Subject stated that they were experiencing technical difficulties with verifying their identity and that the Respondent had informed them that their account was temporarily suspended. The Data Subject was not satisfied with the Respondent's response.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and

- b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Data Subject’s account was active again, and that they could now access their personal data through the Respondent’s self-service tools. In the circumstances, the Respondent took the following action:
 - a. The Respondent wrote to the Data Subject directly, confirming that their account was active.
 - b. The Respondent provided instructions to the Data Subject on how they could access their data using the Respondent’s self-service tools.
8. On 7 February 2022, the DPC outlined the Data Subject’s complaint to the Respondent, providing it with a copy of the correspondence exchanged between the Data Subject and the Respondent. The DPC noted the Data Subject indicated that they could usually access their personal data using the Respondent’s self-service tools, but that on this occasion, they were being redirected to an identity verification window upon login. On 2 March 2022, the Respondent responded to the DPC and confirmed it had communicated directly with the Data Subject on the same date, informing them that their account was now active. The Respondent also provided instructions to the Data Subject on how they could access their data using the Respondent’s self-service tools.
9. On 20 April 2022, the DPC wrote to the Data Subject outlining the information provided by the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action.

The DPC did not receive any further communication from the Data Subject, and, accordingly, the complaint has been deemed to have been amicably resolved.

10. On 14 September 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Commission Nationale de l'Informatique et des Libertés pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 14 July 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Commission Nationale de l’Informatique et des Libertés (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 23 July 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject’s account was suspended by the Respondent. The Data Subject stated in their complaint that they subsequently submitted an erasure request to the Respondent under Article 17 GDPR by email on 25 April 2021.
 - b. The Data Subject asserted that they received an email from the respondent on 1 May 2021. In this email, the Respondent advised the Data Subject that following a violation of the Respondent’s Terms of Use, the Respondent had suspended the Data Subject’s account on 10 March 2021 and as part of that suspension, certain data would be retained in line with the Respondent’s retention policies.
 - c. The Data Subject was dissatisfied with the response received from the Respondent and believed that the Respondent had not fulfilled their request for erasure.
 - d. As the Data Subject was not satisfied with the response received from the Respondent regarding the concerns raised, the Data Subject lodged a complaint with the recipient supervisory authority.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:

- a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject matter of the complaint. Further to that engagement, it was established that the Respondent had suspended the Data Subject’s account and following this suspension, it had retained the Data Subject’s personal data. According to the Respondent, the retention of this data was in line with the Respondent’s data retention policy. Following engagement between the Respondent and the DPC, the Respondent provided the DPC with the following information in respect of the complaint:
 - a. The Respondent agreed to conduct a fresh review of the Data Subject’s suspension.
 - b. Following this review, the Respondent asserted that, due to the nature and volume of the violations by the Data Subject, they were not in a position to lift the suspension of the account.
 - c. In the circumstances, the Respondent offered to provide more information to the Data Subject in relation to the Respondent’s practices.
8. The DPC’s letter outlining the information provided by the Respondent issued to the Data Subject on 7 July 2022 via the Recipient SA. Within its letter to the Data Subject, the DPC noted that the Respondent’s reply attempted to address the data protection concerns set out in the complaint.

9. The DPC requested that the Data Subject notify it, within a specified timeframe, if they were not satisfied with the information provided by the Respondent, so that the DPC could further review their complaint. On 13 September 2022, the Recipient SA confirmed that no response had been received from the Data Subject.
10. On 06 October 2022 and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner
Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF INTERNAL EDPB DOCUMENT 06/2021 ON
THE PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS, ADOPTED 18 NOVEMBER 2021**

Dated the 2nd day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 3 September 2020, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission ("the **DPC**") concerning MTCH Technology Services Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 18 July 2020, requesting access to their personal data, in order to understand what personal data the Respondent processed in relation to them, along with the reason for their account suspension.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to Internal EDPB Document 06/2021 on the practical implementation of amicable settlements, adopted on 18 November 2021 ("Document 06/2021"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

- 7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject's account was disabled due to a breach of the Respondent's Terms of Use and Community Guidelines, but that the Respondent was willing to reactivate the Data Subject's account if they agreed to abide by its Terms of Use and Community Guidelines in future. In the circumstances, the Respondent took the following actions:
 - a. the Respondent agreed to reactivate the Data Subject's account; and
 - b. the Respondent offered to assist the Data Subject in relation to their access request, if they still wished to receive a copy of their personal data following the reactivation of their account.
- 8. On 7 July 2021, the DPC outlined the Data Subject's complaint to the Respondent. The DPC noted that the Data Subject's account had been disabled, and they were concerned that they had no means to withdraw their consent for the Respondent's processing of their personal data. On 21 July 2021, the Respondent replied to the DPC, and confirmed that the Data Subject's account was disabled due to a breach of its Terms of Use and Community Guidelines. The Respondent also provided the DPC with a summary of its interaction with the Data Subject regarding their access request. The Respondent explained that it had requested that the Data Subject verify their identity, however, the Data Subject had refused to provide sufficient information to verify their identity. The Respondent also stated that it had not retained any personal data based on the Data Subject's consent. However, the Respondent confirmed that it had conducted a review of the decision to disable the Data Subject's account and it concluded that it would be willing to reactivate the Data Subject's account, once they agreed to abide by its Terms of Use and Community Guidelines. The Respondent stated that it remained willing to provide the Data Subject with a copy of their personal data, if they were still interested in receiving it, once the Data Subject verified their identity.
- 9. The DPC subsequently wrote to the Data Subject on 27 August 2021, informing them of the Respondent's proposal. On 1 September 2021, the Data Subject responded to the DPC, and agreed to the Respondent's proposal to regain access to their account, but stated that they would not provide any additional personal data in order to do so. On 9 November 2021, the DPC informed the Respondent that the Data Subject had indicated that they accepted its proposal to regain access to their account.

10. On 16 November 2021, the Respondent confirmed to the DPC that it had written to the Data Subject to inform them that their account ban had been lifted in light of their acceptance of its proposal. The Respondent also stated that it had reiterated its offer to assist the Data Subject in relation to their access request. On 26 November 2021, the DPC wrote to the Data Subject. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2021, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2021 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 6th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 12 February 2022, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject submitted an access request to the Respondent, following receipt of notification that their Messenger account had been suspended.
 - b. The Data Subject was dissatisfied with the response of the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent being, in this case, an individual consumer and a service provider; and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Data Subject's Messenger account was currently deactivated, but that the Respondent could provide the Data Subject with access to their personal data via a download link, if the Data Subject could provide the Respondent with a secure email address. In the circumstances, the Respondent took the following actions:
 - a. The Respondent agreed to grant the Data Subject access to their personal data, once the Data Subject had provided a secure email address.
8. On 30 June 2022, the DPC wrote to the Respondent, outlining the Data Subject's complaint. In its correspondence to the Respondent, the DPC noted that, due to limitations of Messenger-only accounts, the Data Subject had initially reached out to the Respondent's support via their child's Facebook account. The Data Subject also requested that the ID they provided to the Respondent at the time of making their original access request be deleted by the Respondent. The DPC provided the Respondent with copies of the correspondence supplied by the Data Subject.
9. On 29 July 2022, the Respondent responded to the DPC. The Respondent confirmed that the Data Subject's account was deactivated, but that it would be able to provide the Data Subject with a URL to download a copy of their personal data, provided the Data Subject could supply it with a secure e-mail address. The Respondent also confirmed that the ID that had been provided by the Data Subject at the time of their access request had been deleted in accordance with its retention policies.
10. On 2 August 2022, the DPC wrote to the Data Subject, asking them to provide a secure e-mail address that could be shared with the Respondent. The DPC noted that once the secure e-mail was shared, the Respondent would then be able to provide them with a URL containing their requested personal data. On the same date, the Data Subject provided their preferred secure e-mail address to the DPC.
11. On 8 August 2022, the DPC wrote to the Respondent, providing it with the secure e-mail address supplied by the Data Subject. In its correspondence to the Respondent, the DPC asked it to write to the Data Subject directly, and to notify the DPC once the data had been provided to the Data Subject. On 22 August 2022, the Respondent shared a copy of the correspondence

sent directly to the Data Subject with the DPC. On 23 August 2022, the DPC wrote to the Data Subject, providing them with a copy of the correspondence received from the Respondent. In its letter to the Data Subject, the DPC noted that the URL provided by the Respondent was time-sensitive, and was due to expire on the same day. The DPC asked the Data Subject to confirm whether they were able to successfully access their personal data. On the same date, the Data Subject confirmed to the DPC they were able to access their personal data. In the circumstances, the DPC asked the Data Subject to notify it, within one month if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Microsoft Ireland Operations Limited.

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

RECORD OF AMICABLE RESOLUTION FOR THE PURPOSE OF EDPB GUIDELINES 06/2022 ON THE PRACTICAL IMPLEMENTATION OF AMICABLE SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 10 May 2021, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission (“the **DPC**”) concerning Microsoft Ireland Operations Limited (“the **Respondent**”).
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject contacted the Respondent on 27 March 2020 and submitted a delisting request pursuant to Article 17 GDPR. The URLs at issue are newspaper articles that relate to the Data Subject’s 2019 criminal conviction for the offence of indirect corruption. This conviction occurred in the Slovak Republic, where the payment of the financial penalty effectively eradicates the conviction and the perpetrator is treated as if they had never been convicted.
 - b. The Data Subject was not satisfied with the response received from the Respondent. The Respondent stated that there was an important public interest involved in accessing this information and as the content was accurate, it should be in the public domain.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Data Subject, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).

6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:
 - a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
 - b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject-matter of the complaint. In the circumstances, the Respondent took the following actions:
 - a. The Respondent agreed to re-evaluate the Data Subject’s delisting request; and
 - b. The Respondent agreed to delist the complained of URLs.
8. On 4 October 2021, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC provided the Respondent with a list of the complained of URLs and the necessary complaint documentation to assist it with its examination of the complaint. The DPC requested that the Respondent outline the reason why the Data Subject’s delisting request was refused.
9. On 18 October 2021, the Respondent responded to the DPC. The Respondent stated that it re-reviewed the Data Subject’s delisting request and maintained its position that the URLs should not be blocked under the Article 17 GDPR Right to Be Forgotten.
10. The DPC subsequently engaged in communications with the Slovakian Data Protection Authority, including on the effect the payment of a financial penalty has on the status of a conviction under Slovakian law, and held detailed discussions with the Respondent concerning the complaint. On 14 February 2022, the Respondent informed the DPC that following a re-evaluation of the Data Subject’s request, it would now delist the URLs.
11. The DPC wrote to the Data Subject on 24 February 2022. When doing so, the DPC noted that, as the URLs which were the subject matter of the complaint had been delisted, the dispute between the Data Subject and Respondent appeared to have been resolved. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not

receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.

12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:



Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Luxembourg Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Luxembourg Data Protection Authority (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 26 October 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject made an access request, pursuant to Article 15 GDPR, following the disablement of their account.
 - b. The Respondent provided the Data Subject with a data package. However, this did not provide any information regarding the account disablement.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that, due to human error by a customer care agent, the account was incorrectly disabled. In the circumstances, the Respondent took the following actions:
 - a. The Respondent contacted the Data Subject directly and confirmed that their account was reactivated; and
 - b. The Respondent offered to aid the Data Subject with any further concerns relating to their account.
8. On 13 December 2021, the DPC outlined the Data Subject's complaint to the Respondent noting that they requested a copy of all their personal data stored through the link on the Respondent's website in order to understand the reason for their account disablement. The DPC noted that the Data Subject did receive a data package from the Respondent, however, this did not include any information in relation to their account disablement.
9. On 30 December 2021, the Respondent responded to the DPC. The Respondent informed the DPC that following a review it found that, due to human error by a customer care agent, the Data Subject's account was incorrectly disabled. The DPC outlined the Respondent's response to the Data Subject on 11 February 2022, which the Recipient SA forwarded on 10 March 2022. The DPC noted in this correspondence that the account was now reactivated. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
10. On 9 August 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.

11. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:

- a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
- b. The agreed resolution is such that the object of the complaint no longer exists; and
- c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.

13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tom Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the French Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning MTCH Technology Services Limited

**Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018**

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 15th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the French Data Protection Authority (“the **Recipient SA**”) concerning MTCH Technology Services Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 22 February 2022.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject was dissatisfied with the Respondent’s response to their Article 13 GDPR request for information and their Article 15 GDPR access request, following the suspension of their account.
 - b. The Data Subject was also dissatisfied with portions of MTCH’s updated Terms of Service and Privacy Policy, insofar as it related to the retention of personal data of individuals banned from the Tinder service.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, the Respondent conducted a fresh review of the Data Subject’s account ban and decided to lift it. In the circumstances, the Respondent took the following actions:
 - a. The Respondent contacted the Data Subject directly, informing them that their account ban had been lifted; and
 - b. The Respondent provided the DPC with information relating to the Data Subject’s concerns with respect to any automated profiling and processing of personal data which may result in an account being banned. The Respondent also provided information on the duration for which the Respondent retains personal data relating to banned accounts.
8. On 20 May 2022, the DPC outlined the Data Subject’s complaint to the Respondent. The DPC noted that the Data Subject was dissatisfied with portions of the Respondent’s updated Terms of Service and Privacy Policy, insofar as it related to the retention of personal data of individuals banned from the Tinder service. The DPC also noted that the Data Subject’s Tinder account had been banned by the Respondent for a violation of its Terms of Use or Community Guidelines.
9. The DPC informed the Respondent of the Data Subject’s concerns regarding automated decision making, and their assertion that the Respondent’s retention of their data for ‘as long as necessary’ as a result of their account ban is without proper oversight, and could lead to the Respondent retaining personal data indefinitely. The DPC highlighted that the Respondent had previously confirmed to the Data Subject that their account was banned from its service due to a violation of its Terms of Use or Community Guidelines. The DPC noted that the Respondent had stated in this correspondence to the Data Subject that it did not offer an appeal process at that time, and that the Data Subject’s account would remain banned, and furthermore they would not be able to create a new Tinder profile using their Facebook account and/or phone number.

10. On 20 June 2022, the Respondent responded to the DPC. The Respondent stated that its Tinder Trust and Safety team had reviewed the Data Subject's account again and found that it had no record of an appeal process being conducted. However, the Respondent confirmed that it had decided to lift the ban on the Data Subject's account, allowing the Data Subject to create a new account.
11. The Respondent also provided information on their account banning practices and their retention policies. The Respondent clarified that when an account is deleted or banned, the vast majority of personal data is deleted, and that only limited personal data is retained to ensure the safety of its users and protect their vital interests. The Respondent explained that this data is retained for 5 years, and then subsequently deleted. On 8 August 2022, the DPC wrote to the Data Subject via the Recipient SA outlining the information received from the Respondent. In the circumstances, the DPC asked the Data Subject to notify it, within 2 months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
12. On 1 November 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
13. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

14. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
15. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Data Protection Commission pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited (formerly Facebook Ireland Limited)

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to
Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of
amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0
(ADOPTED ON 12 MAY 2022)**

Dated the 9th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 31 May 2021, [REDACTED] ("the **Data Subject**") lodged a complaint pursuant to Article 77 GDPR directly with the Data Protection Commission ("the **DPC**") concerning Meta Platforms Ireland Limited ("the **Respondent**").
2. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject emailed the Respondent on 31 March and 24 April 2021. In these emails, the Data Subject made a request under Article 17 of the GDPR for the erasure of their personal data, including their accounts on both the Facebook and Instagram platforms.
 - b. On 31 May 2021, the Data Subject informed the DPC that they had not received any response from the Respondent, and as such requested that the DPC pursue the matter further.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 ("the **2018 Act**"), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC's experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual and a service provider; and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 (“**Document 06/2022**”), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject and Respondent in relation to the subject matter of the complaint. Further to that engagement, the Respondent advised the DPC that upon reviewing the complaint, the Data Subject’s accounts had been disabled for violations of the Respondent’s Terms of Service and Community Guidelines.
8. On 04 August 2022, in an effort to amicably resolve the complaint in question, the DPC contacted the Respondent seeking their cooperation in removing the personal data in question.
9. On 26 August 2022, the Respondent informed the DPC that upon further review by their specialist team, there was evidence to suggest that the Data Subject’s accounts on both the Facebook and Instagram platforms may have been compromised. On this basis, the Respondent agreed to proceed with the deletion of the accounts.
10. The DPC’s letter outlining the information provided by the Respondent issued to the Data Subject on 22 September 2022. When doing so, the DPC noted that the Respondent had agreed to the erasure of their accounts. In the circumstances, the DPC asked the Data Subject to notify it, within a specified timeframe, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. In circumstances where the subject matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

12. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;

- b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
13. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner
Data Protection Commission.

In the matter of the General Data Protection Regulation

DPC Complaint Reference: [REDACTED]

IMI Complaint Reference Number: [REDACTED]

In the matter of a complaint, lodged by [REDACTED] with the Hamburg Data Protection Authority pursuant to Article 77 of the General Data Protection Regulation, concerning Meta Platforms Ireland Limited

Record of Amicable Resolution of the complaint and its consequent withdrawal pursuant to Section 109(3) of the Data Protection Act, 2018

Further to the requirements of EDPB Guidelines 06/2022 on the practical implementation of amicable settlements Version 2.0 (adopted on 12 May 2022)

**RECORD OF AMICABLE RESOLUTION FOR THE
PURPOSE OF EDPB GUIDELINES 06/2022 ON THE
PRACTICAL IMPLEMENTATION OF AMICABLE
SETTLEMENTS VERSION 2.0, ADOPTED 12 MAY 2022**

Dated the 13th day of December 2022



Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, Ireland

Background

1. On 6 April 2020, [REDACTED] (“the **Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Hamburg Data Protection Authority (“the **Recipient SA**”) concerning Meta Platforms Ireland Limited (“the **Respondent**”).
2. In circumstances where the Data Protection Commission (“the **DPC**”) was deemed to be the competent authority for the purpose of Article 56(1) GDPR, the Recipient SA transferred the complaint to the DPC on 9 April 2021.

The Complaint

3. The details of the complaint were as follows:
 - a. The Data Subject was unable to access their Facebook account following a password change, as they no longer had access to the e-mail address and phone number used to create their Facebook account. The Data Subject subsequently submitted an access request to the Respondent on 2 February 2020, seeking access to their personal data.
 - b. The Data Subject was not satisfied with the response received from the Respondent.

Action taken by the DPC

4. The DPC, pursuant to Section 109(4) of the Data Protection Act, 2018 (“the **2018 Act**”), is required, as a preliminary matter, to assess the likelihood of the parties to the complaint reaching, within a reasonable time, an amicable resolution of the subject-matter of the complaint. Where the DPC considers that there is a reasonable likelihood of such an amicable resolution being concluded between the parties, it is empowered, by Section 109(2) of the 2018 Act, to take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.
5. Following a preliminary examination of the material referred to it by the Recipient SA, the DPC considered that there was a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint. The DPC’s experience is that complaints of this nature are particularly suitable for amicable resolution in circumstances where there is an obvious solution to the dispute, if the respondent is willing to engage in the process. In this regard, the DPC had regard to:
 - a. The relationship between the Data Subject and Respondent (being, in this case, an individual consumer and a service provider); and
 - b. The nature of the complaint (in this case, an unsuccessful attempt by the Data Subject to exercise their data subject rights).
6. While not relevant to the assessment that the DPC is required to carry out pursuant to Section 109(4) of the 2018 Act, the DPC also had regard to EDPB Guidelines 06/2022 on the practical

implementation of amicable settlements Version 2.0, adopted on 12 May 2022 ("Document 06/2022"), and considered that:

- a. the possible conclusion of the complaint by way of amicable resolution would not hamper the ability of the supervisory authorities to maintain the high level of protection that the GDPR seeks to create; and that
- b. such a conclusion, in this case, would likely carry advantages for the Data Subject, whose rights under the GDPR would be vindicated swiftly, as well as for the controller, who would be provided the opportunity to bring its behaviour into compliance with the GDPR.

Amicable Resolution

7. The DPC engaged with both the Data Subject (via the Recipient SA) and Respondent in relation to the subject-matter of the complaint. Further to that engagement, it was established that the Respondent had contacted the Data Subject directly to assist them in regaining access to their Facebook account. In the circumstances, the Respondent agreed to take the following actions:
 - a. The Respondent agreed to have its specialist team reach out to the Data Subject directly to assist them with regaining access to their account; and
 - b. The Respondent confirmed to the DPC that should the Data Subject have any further issues with regaining access to their account and personal data, then it would assist them further.
8. In the Data Subject's access request to the Respondent, the Data Subject outlined that, after a successful password change, they were still unable to log into their account. The Data Subject informed the Respondent that they no longer had access to the e-mail address and phone number used to create their Facebook account. Upon receipt of the Data Subject's complaint from the Recipient SA, the DPC engaged further with the Data Subject via the Recipient SA, in order to assess the complaint and fully understand the Data Subject's desired outcome, as it was unclear from the received correspondence whether or not the Respondent had responded to the Data Subject's initial access request. The DPC asked the Recipient SA to provide copies of correspondence between the Data Subject and the Respondent, in order to fully assess the complaint and to progress the complaint further. On 29 April 2022, the DPC outlined the Data Subject's complaint to the Respondent. The DPC requested that the Respondent review the complaint documentation provided, and write to the Data Subject directly, responding to their access request.
9. On 25 May 2022, the Respondent responded to the DPC. The Respondent noted that it had previously contacted the Data Subject directly at their alternative email address on 1 April 2022, after the Data Subject had provided the Respondent with the ID documentation necessary to verify their identity. The Respondent explained that it had sent the Data Subject a password reset link on this date, which was resent to them on 28 April 2022, at their request.

However, the Respondent confirmed that following a review of its internal systems, it appeared that the Data Subject did not make use of the password reset link within the 7 day period specified and, as such, the link expired. In its correspondence to the DPC, the Respondent stated that its specialist team would again reach out to the Data Subject to assist them in regaining access to their account and accessing their personal data. The Respondent stated that once the Data Subject had regained access to their account they would be able to use its self-serve access tools to download a copy of their personal data. The Respondent outlined that if the Data Subject was experiencing any issues with accessing the password link once it is received then it could assist the Data Subject further.

10. On 24 July 2022, the DPC wrote to the Data Subject via the Recipient SA, outlining the response received from the Respondent. The DPC highlighted to the Data Subject that, once the Respondent contacted them, they would need to follow the instructions provided, and use the password link before it expires, in order to reset their password. In the circumstances, the DPC asked the Data Subject to notify it, within two months, if they were not satisfied with the outcome, so that the DPC could take further action. The DPC did not receive any further communication from the Data Subject and, accordingly, the complaint has been deemed to have been amicably resolved.
11. On 25 October 2022, and in light of the foregoing, the DPC wrote to the Recipient SA noting that the DPC considered the complaint to have been amicably resolved and withdrawn in accordance with section 109(3) of the Act and that it would conclude the case and inform the Respondent.
12. In circumstances where the subject-matter of the complaint has been amicably resolved, in full, the complaint, by virtue of Section 109(3) of the 2018 Act, is deemed to have been withdrawn by the Data Subject.

Confirmation of Outcome

13. For the purpose of Document 06/2022, the DPC confirms that:
 - a. The complaint, in its entirety, has been amicably resolved between the parties concerned;
 - b. The agreed resolution is such that the object of the complaint no longer exists; and
 - c. Having consulted with the supervisory authorities concerned on the information set out above, as required by Document 06/2022 the DPC has now closed off its file in this matter.
14. If dissatisfied with the outcome recorded herein, the parties have the right to an effective remedy by way of an application for judicial review, by the Irish High Court, of the process applied by the DPC in the context of the within complaint.

Signed for and on behalf of the DPC:

A handwritten signature in black ink, appearing to read "Tony Delaney".

Deputy Commissioner

Data Protection Commission