

**Deliberation No 42/RECL15/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.646 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185217**

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: [REDACTED]) via IMI in accordance with Article 61 procedure - 185217.
2. The complaint was lodged against the controller [REDACTED] ([REDACTED]) who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant requested erasure and in his opinion [REDACTED] didn't sufficiently process it, as his account is only blocked and not deleted.”

**Deliberation No 42/RECL15/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.646 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185217**

4. In essence, the complainant asks the CNPD to request [REDACTED] to close his account and delete all his personal data.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*";
9. In accordance with Article 17 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 (...)*";
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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*";

**Deliberation No 42/RECL15/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.646 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185217**

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:

- The complainant's request to close his account was completed in the same month as the request. Subsequent to the complainant's request, [REDACTED] sent e-mails to the complainant to notify that his account was blocked and that he should log in again to unblock his account. [REDACTED] further stated that these e-mails were sent in error, and [REDACTED] had already identified the technical source for this error and had addressed it.
- [REDACTED] informed the complainant of the completion of his erasure request.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 of the GDPR.

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted the supervisory authority Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.



**Deliberation No 42/RECL15/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.646 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185217**

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.646 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 9 June March 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



Deliberation No 84/RECL30/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.035 lodged against the company via IMI Article 61 procedure 161989

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: [REDACTED]) via IMI in accordance with Article 61 procedure - 161989.
2. The complaint was lodged against the controller [REDACTED] ([REDACTED]), who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant wants his seller account to be deleted as he no longer acts as a seller. The seller has a new e-mail address, so he is no longer able to access it.”
4. In essence, the complainant asks the CNPD to request [REDACTED] to close his [REDACTED] seller account and delete any related personal data.

Deliberation No 84/RECL30/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.035 lodged against the company via IMI Article 61 procedure 161989

5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his request for erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 17 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 (...)*";
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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*";

Deliberation No 84/RECL30/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.035 lodged against the company via IMI Article 61 procedure 161989

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- The complainant requested the closure of his [REDACTED] seller account in April and May 2020.
- As the complainant's requests originated from his new email address and not from the email address linked with his [REDACTED] seller account, [REDACTED] was initially not able to comply with the requests due to the requirement to verify his identity.
- In addition, the complainant's [REDACTED] seller account was deactivated because of outstanding debts which needs to be cleared before [REDACTED] could process the request.
- [REDACTED] had then reached out to the complainant to solve the issue and then proceeded with the closure and deletion of his [REDACTED] seller account.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 of the GDPR.

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted the supervisory authority of Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.



Deliberation No 84/RECL30/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.035 lodged against the company via IMI Article 61 procedure 161989

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.035 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 22 September 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



**Deliberation No 85/RECL31/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.347 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174363**

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: [REDACTED]) via IMI in accordance with Article 61 procedure - 174363.
2. The complaint was lodged against the controller [REDACTED], who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant submits that he has requested access to his personal data according to Article 15 of the GDPR. Due to the fact that his customer account is blocked, he could not claim or obtain the requested information by logging into his customer account. He therefore contacted the controller’s customer support department and received notification from there that verification of the applicant’s person required verification by telephone and he was asked to provide a telephone number so that a callback could be

**Deliberation No 85/RECL31/2023 of 22 September 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.347 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174363**

made. He told his telephone number several times to the controller but never received a call back. As a result, the right of access has not been fulfilled."

4. In essence, the complainant asks the CNPD to request [REDACTED] to grant him access to his data.
5. The complaint is therefore based on Article 15 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right of access.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 15 of the GDPR "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (...)*";
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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";

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:
- It researched the case and found out that [REDACTED]'s response of 3 January 2021 to its request for a telephone number and timeslot was not routed to the responsible team.
 - This was due to [REDACTED]'s account being suspended for outstanding amounts.
 - Therefore, the verification call did not take place and consequently the verification process was not completed.
 - Upon receipt of the CNPD's letter it contacted [REDACTED] via phone on 12 May 2021 and the verification was successful.
 - The controller then sent [REDACTED] the personal data relating to his email account on a password protected USB stick. The controller also started proceeding with [REDACTED]'s request for account closure and data deletion.
 - On a subsidiary note, the controller also offered [REDACTED] a gift card in acknowledgement of the poor experience he had in this case and had written off the debt on his account. The controller also informed the CNPD that it intended to retrain the relevant customer service associates on how to recognize data subject access related requests and related verification requests, and will also continue to review this complaint internally in order to identify opportunities to ensure [REDACTED]'s experience is not repeated.



**Deliberation No 85/RECL31/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.347 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174363**

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right of access request, in accordance with Article 15 of the GDPR.
15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
16. The CNPD then consulted the supervisory authority of Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.347 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 22 September 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner



**Deliberation No 85/RECL31/2023 of 22 September 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.347 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174363**

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Final decision

The present decision refers to the case/complaint of [REDACTED], lodged with the supervisory authority of Denmark (national reference 2018-31-0530) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 58117.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED”]), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

In the original IMI case, the complainant stated that:

- (1) it was not possible to access his personal data linked with all the [REDACTED] [REDACTED] in a single request (a separate request has to be done separately on each [REDACTED]), and that
- (2) the website [REDACTED] did not offer the data subjects the possibility to access their personal data.

The complaint is thus mainly based on Article 15 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1(a) GDPR, in particular as regards to the possibility for data subjects to obtain their personal data linked with all [REDACTED] [REDACTED] in a single request.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has demonstrated that:

- As for point (1), [REDACTED] was already, back in 2018, in the process of putting in place a technical solution allowing data subjects to access their personal data linked with all their [REDACTED] [REDACTED] accounts in a single request. Thus, it is thus now possible for every [REDACTED] customers to request their personal data from all [REDACTED] in one single request.
- As for point (2), unlike for the [REDACTED] (e.g., [REDACTED] [REDACTED]), the personal data processed in the context of the website [REDACTED] are controlled by a U.S. based company ([REDACTED]), for which the CNPD is not the competent supervisory authority. In addition, the website

[REDACTED] has also implemented, in the meantime, a tool for customers to access their personal data linked with their account on [REDACTED]. This point has been confirmed by the complainant who indicated that this issue has been solved satisfactorily.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and the CNPD has consulted the supervisory authority of Denmark to determine whether the case could be closed. The CNPD and the supervisory authority of Denmark agreed that, in view of the above, no further action or additional measures are needed and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294504).

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

For the National Data Protection Commission

Final decision

The present decision refers to the complaint of [REDACTED] lodged with the supervisory authority of Austria (national reference D130.270) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 70691.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED”]), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

In the initial complaint on IMI, the representative (lawyer) of the complainant sent a copy of the letter in which he stated that the controller did not react to the access request as per Article 15 GDPR. More precisely, he explained that the complainant had an insurance relationship with the controller, that the complainant exercised his right to access with e-mail from 29.10.2019 and that the controller did not react to the request. The complainant requested in particular specific documents as the insurance application, the original policy and the policy conditions relating to the contract, the repurchase statement (etc).

The complaint is thus based on Article 15 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a), in particular as regards the right of access of [REDACTED] to his personal data processed by the company, in particular by the Austrian branch named [REDACTED]. The CNPD requested [REDACTED] to provide (1) to the CNPD with the reasons why [REDACTED] has not been informed, within one month, of the actions taken for his access request and (2) to act on [REDACTED] access request, or provide CNPD with the reasons that would justify not to act on this access request.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, the controller has given the following explanations:

- The company [REDACTED] ("[REDACTED]") has been recently set-up in Luxembourg in order to allow the [REDACTED] ("[REDACTED"]"), [REDACTED], to continue to serve its in force European insurance portfolio post Brexit under EU passporting rules. [REDACTED] ("[REDACTED"]"), through its legacy [REDACTED] brand, previously distributed life insurance business to customers in the European Economic Area (EEA) outside the United Kingdom. The principal markets were [REDACTED]
[REDACTED].
- Incorporated on [REDACTED], [REDACTED] obtained a life insurance licence from the Luxembourg regulator (Commissariat aux Assurances) on [REDACTED].
- Effective [REDACTED], the in force European insurance portfolio transferred from [REDACTED] to [REDACTED] (the "Transfer"). For the avoidance of doubt, any residual current or future liabilities relating to closed (i.e. not in force) policies remained with [REDACTED].
- The policy of [REDACTED].., a [REDACTED], had started on 23 July 2007, was assigned on 16 February 2016 and surrendered by the assignee on 8 August 2018. A revocation request was made on 19 December 2018 and rejected on 18 January 2019. On 29 March 2019, this policy was no longer in force and so any residual liabilities therefore remain with [REDACTED].
- [REDACTED] indeed received the Data Subject Access request ("DSAR") via a letter dated 21 November 2018 but the DSAR request was accidentally closed rather than processed. No communication has been sent to [REDACTED] or his lawyer and no contact has been made by the lawyer requesting the DSAR until the receipt of CNPD letter. According to [REDACTED], measures have been taken at pace to understand the exact root cause and ensure this does not happen again.
- [REDACTED] then confirmed that it had acted on the DSAR request and that the relevant data pack was posted using registered mail.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and that the controller has taken quick appropriate measures to satisfy the complainants' right of access.

As the complaint had only a limited personal impact, the CNPD has consulted the supervisory authority of Austria to determine whether the case could be closed. The CNPD and the supervisory authority of Austria agreed that, in view of the above, no further action or additional measures are needed and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise or its investigative and corrective powers regarding the data processing activities in the event of a new complaint.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294704).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of █, lodged with the supervisory authority of Austria (D130.288) and submitted to the Luxembourg supervisory authority via IMI under Article 61 procedure 73146.

The complaint was lodged against the controller █. (hereinafter “█”), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial complaint on IMI stated that the complainant requested the cancellation of her test offer and the deletion of her personal data from █ several times by e-mail. She also claimed that her request was apparently not granted.

The complaint is thus based on Article 17 GDPR.

Based on said complaint, the CNPD requested the controller to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) GDPR, in particular as regards to her deletion request.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, the legal representative of the controller informed the CNPD that the data of the complainant was indeed erased on request back in 2019, but that due to an human error, the complainant was not informed thereof. A copy of the new information letter was then send to the CNPD.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and/or the exercised right has been attended.

As the complaint has only a limited personal impact, the CNPD has consulted the supervisory authority of Austria to determine whether the case could be closed. The CNPD and the supervisory authority of Austria agreed that, in view of the above, no further action or additional measures are needed and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 293747).

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

For the National Data Protection Commission

Final decision

The present decision refers to the complaint of [REDACTED], lodged with the supervisory authority of Germany, Hamburg, (national reference D51/2470/2018) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 57757.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED”]), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

“A German client of the [REDACTED] [REDACTED] has requested Access to his personal data. [REDACTED] did not send the data directly but sent him information on how to download it. The complainant is convinced that this way is not reasonable.”

The complaint is thus based on Article 15 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1(a) GDPR, in particular as regards the reasons why [REDACTED] advised [REDACTED] to log into his [REDACTED] account and then go on an [REDACTED] webpage where he could request his personal data, instead of complying with the access request directly. The CNPD also requested [REDACTED] to comply with the complainant’s data access request.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has demonstrated that:

- [REDACTED] accepts data subject access requests through various channels but needs to properly identify the requestor as holder of the respective customer account in order to make sure to only disclose personal data to the respective data subject.
- The easiest way for the customer to identify themselves, is indeed to log into their [REDACTED] account and submit their request via the designated contact form. However, if the customer does not want this, [REDACTED] clearly stated that it will also comply with other ways of identification.

- In the case at hand, [REDACTED] did not refuse the subject access request but [REDACTED] was not able to properly identify [REDACTED] on the basis of his e-mail and therefore asked him to preferably use the designated contact form in his customer account.
- Following receipt of the CNPD letter regarding [REDACTED]'s complaint, [REDACTED] contacted the customer asking him to confirm that he is requesting access to his personal data.
- [REDACTED] informed the CNPD that [REDACTED] confirmed that he was requesting access to his personal data and that [REDACTED] was going to work on his data set immediately and make it available to [REDACTED] once completed.

Thus, based on the information that was provided, the CNPD is of the view that the controller has taken appropriate measures to satisfy the complainants' right of access pursuant to Article 15 of the General Data Protection Regulation.

As the complaint has only a limited personal impact, the CNPD has consulted the supervisory authority of Hamburg (Germany) to determine whether the case could be closed. The CNPD and the supervisory authority of Hamburg (Germany) agreed that, in view of the above, no further action or additional measures are needed and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294009).

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

For the National Data Protection Commission

Final decision

The present decision refers to the complaint of [REDACTED] lodged with the supervisory authority of Germany, Rhineland-Palatinate, (national reference 4.02.19.092) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 66577.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED”]), which has its main establishment in Luxembourg. Pursuant to Article 56 of the GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

“The complainant alleges that he could not pay by [REDACTED] but only by direct debit. Consequently, he immediately interrupted the procedure and did not enter his banking details. However, the following day the parcel arrived that he has not ordered and there was also a debit from his bank account. Thus, the complainant wonders how [REDACTED] got his data, especially his banking details. Apparently, the complainant contacted [REDACTED] and [REDACTED] apologised but nevertheless, the complainant is not happy with the situation.”

The complaint is thus based on Article 15 of the GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) of the GDPR, in particular further information regarding the origin of the personal data processed by [REDACTED] and, more specifically, how [REDACTED] obtained his payment data.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has demonstrated that:

- The complainant opened a customer account related to the e-mail address [*known by the CNPD*] and registered his bank account details on 16 September 2016. He subsequently subscribed to a “[REDACTED] membership” and placed four orders, including the order described in the complaint.
- For all four orders, the records show that [REDACTED] selected direct debit as the preferred payment option, which entailed the use of the bank account details [REDACTED] had previously provided.

- For the order described in the complaint, the complainant clicked to [REDACTED] to complete the order; otherwise the order number would not have been generated. In general, [REDACTED] customers receive an order confirmation via e-mail and have the option to cancel any order after placing it.
- The complainant did not cancel the order and did not send any other message to [REDACTED] so the order was processed and shipped.
- [REDACTED] is not an accepted payment method on [REDACTED]. This is explicitly stated on the customer help page concerning available payment options.

Thus, based on the information that was provided, the CNPD did not identify any infringement by the controller of the obligations set out in Regulation (EU) 2016/679 (GDPR).

In light of the above, the CNPD has consulted the supervisory authority of Rhineland-Palatinate (Germany) to determine whether the case could be closed. The CNPD and the supervisory authority of Rhineland-Palatinate (Germany) agreed that, in view of the above, no further action is required and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294013).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED] lodged with the supervisory authority of Germany, Bavaria, (national reference LDA-1085.4-8170/18-I) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 61900.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED]”) which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

“[REDACTED] did not process or did not fully process the complainant's request regarding the access to the personal data relating to him that [REDACTED] is processing.”

The complaint is thus based on Article 15 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant's data processing as per Article 58.1 a) GDPR, and in particular to the request by the complainant to access his personal data processed by [REDACTED].

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] informed the CNPD that it was not able to locate the letter of the complainant from 2018 attached to the complaint (and the complainant did not communicate a valid proof of sending either).

[REDACTED] confirmed though that the complainant contacted [REDACTED] customer service in June 2019 requesting information about his data, how [REDACTED] is processing it and in about data that is shared with third parties.

[REDACTED] replied to the complainant's questions, and provided him with the requested information. [REDACTED] also informed the complainant about what data he could further review in his customer account and how he could submit a data subject access request the easiest way by logging in into his customer account and submitting the request via the designated contact form therein. This way he will be properly identified as holder of the respective customer account for which he requests the data set for. However, [REDACTED] did not hear back from the complainant since [REDACTED] last response to him. He did not communicate any further questions regarding the processing of his data, nor complications with or refusal to use the contact form to submit the data subject access

request. [REDACTED] therefore had assumed that the complainant was satisfied with the information provided.

Finally, following receipt of the CNPD's letter regarding the present complaint, [REDACTED] contacted the complainant a second time in order to provide him with the requested data.

Thus, based on the information that was provided, the CNPD is of the view that the controller has taken appropriate measures to satisfy the complainants' right of access, pursuant to Article 15 of the General Data Protection Regulation.

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

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294505).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED] lodged with the supervisory authority of France (national reference 18019666) and submitted to the Luxembourg supervisory authority via IMI under Article 61 procedure 77871.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED]” which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

“The complainant asked [REDACTED] to delete his account from its [REDACTED] platform as well as all information about the books he published. [REDACTED] did not comply with his request. [REDACTED] has answered him that it does not remove the [REDACTED] pages in order to help clients to easily find information about authors they like. [REDACTED] told the complainant that it could only dissociate his email address from the [REDACTED] page. This reply does not seem satisfactory in respect with the deletion request of the complainant.”

The complaint is thus based on Article 17 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1(a) GDPR, in particular as regards the refusal by the controller to remove the complainant’s [REDACTED] page and to erase his books references from [REDACTED]’s websites.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Although the complainant framed his request as an exercise of his rights as a data subject under the GDPR, both GDPR and copyright laws are relevant to defining the scope of [REDACTED] rights and their obligations in this case.

Indeed, under EU copyright law, where a copyrighted work is legally purchased or acquired by another owner, it may subsequently be sold and resold without restriction (see Article 4 of Directive 2001/29/EC of 22 May 2001). The exhaustion of right principle applies to copies of [REDACTED] works legally sold into circulation at his own request. Accordingly, any third-party sellers has the right to resell any of those copies of the Books legitimately acquired, including used copies

of the Books, on [REDACTED] websites via the [REDACTED]. And [REDACTED] indeed offers customers the opportunity to find out-of-print books through [REDACTED], which is similar to a used bookstore and lists a wide selection of titles for customers' reference and convenience. [REDACTED] name is displayed on the [REDACTED] Page and [REDACTED] pages only for informational purposes in association with the Books he has authored. This information was released to [REDACTED] and the public by [REDACTED] for the purpose of commercially trading his Books. [REDACTED] is therefore entitled under copyright law to display [REDACTED] name on the product detail pages and on [REDACTED] Page for purposes of enabling the legitimate, non-infringing sale of [REDACTED]s Books. In particular, although [REDACTED] will no longer fulfil new orders placed for the Books, it remains possible that someone could wish to sell a used copy of the Books on [REDACTED] websites; in that case the [REDACTED] pages would be needed to enable that sale.

Considering its compliance with Article 17 GDPR in the context of [REDACTED] erasure request, the GDPR permits [REDACTED] to continue to process [REDACTED] name for the abovementioned purpose, as no grounds for erasure apply under Article 17(1) GDPR. In particular, the processing of [REDACTED] name for this purpose is still "necessary in relation to the purposes for which [it was] collected or otherwise processed" as contemplated in Article 17(1) a); the accurate identification of Books authored by [REDACTED] and lawfully offered for sale to consumers is an "overriding legitimate ground" for processing as contemplated in Article 17(1)(c); and none of the other grounds set forth in Article 17(1) is relevant in this case.

In addition, [REDACTED] has described the context of making [REDACTED] books available for sale on [REDACTED] and of [REDACTED] claiming of his [REDACTED] page, so that the Supervisory authority/ies can gain a complete understanding of the abovementioned rationale for the subject erasure request:

In October 2014, [REDACTED] registered for the [REDACTED] service and self-published two books for sale on [REDACTED]. In November 2014, another book was also made available for sale on [REDACTED]. (Collectively, the "Books.") He chose to offer the Books in printed physical format and enabled distribution rights on several [REDACTED]. He also accepted terms and conditions under which [REDACTED] granted [REDACTED] a right to use information identifying and describing the Books (e.g., title, author, synopsis) on the [REDACTED] website.

[REDACTED] explains that product detail pages are where customers can go to find information about specific product listings on [REDACTED] so that customers may learn about products offered for sale. Detail pages include all offer details available for a particular product, including offers for new copies as well as used copies which are sold by third party selling partners via the [REDACTED]. On December 8, 2018, [REDACTED] disabled sales rights for the self-published Books, meaning that future sales of new copies of the self-published Books were discontinued. Consistent with the rights granted by [REDACTED], however, information about the Books remained visible on detail pages in order to enable listings of used copies.

[REDACTED] also used [REDACTED] [REDACTED] service. [REDACTED] explains that this service allows authors to claim and enhance the [REDACTED] for their books within [REDACTED]. [REDACTED] pages are one way [REDACTED] organizes its catalog to help customers find titles they are interested in, and can be accessed by clicking on the [REDACTED]. The [REDACTED] page consists of a list of all the books in their store by that [REDACTED]. By claiming the [REDACTED] page

for their books in [REDACTED] authors confirm their identity as the author of their books [REDACTED] [REDACTED], e.g., biographical information, photos, details about book tours [REDACTED]. The author is able to add, modify, and delete this additional information from the author page via the [REDACTED] tools as well as by contacting [REDACTED]. In September 29, 2014, [REDACTED] claimed his [REDACTED] by confirming his identity as the author of the Books through his [REDACTED] Account linked to his email address.

Finally, without prejudice to the explanations above, [REDACTED] has exceptionally and voluntarily resolved [REDACTED] request by removing the detail pages and [REDACTED] [REDACTED] Page from their websites, considering that there are no used copies of the Books currently offered on [REDACTED] websites.

[REDACTED] has also demonstrated that they informed [REDACTED] accordingly by email, and provided the CNPD with a copy of this communication.

Thus, based on the information that was provided, the CNPD is of the view that the controller has taken appropriate measures to satisfy the complainants' right to erasure, pursuant to Article 17 of the General Data Protection Regulation.

The CNPD has consulted the supervisory authority of France to determine whether the case could be closed. The CNPD and the supervisory authority of France agreed that, in view of the above, no further action is required and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294749).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED] lodged with the supervisory authority of Germany, Brandenburg, (national reference 136/18/1621) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 58964.

The complaint was lodged against the controller [REDACTED] (hereinafter [REDACTED]), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

“Data subject alleges that [REDACTED] did not sufficiently gave access to all data and in particular regarding a commercial dispute between [REDACTED] and the complainant.”

The complaint is thus based on Article 15 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) GDPR, in particular to grant the complainant access to his personal data that [REDACTED] is processing regarding the above-mentioned dispute the basis of [REDACTED] claim.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has demonstrated the following:

- The complainant had multiple email addresses associated with his account. Following an in-depth investigation, [REDACTED] records showed that [REDACTED] had not received a data access request from either of the email addresses associated with the complainant, ‘XXX1’ or ‘XXX2’ (*known by the CNPD*).
- With respect to the commercial dispute, [REDACTED] reviews showed that the complainant opened a [REDACTED] complaint. [REDACTED] reached out to the complainant for more information but did not receive a response from him. Thus, the case was closed in favor of the [REDACTED]. Upon closure of the complaint, [REDACTED] automated email, sent on 6 December 2015, advised t [REDACTED] and [REDACTED]

[REDACTED] was then showing as negative. [REDACTED] received the complainant's request for [REDACTED] to provide the reason for the [REDACTED]. The complainant was subsequently sent the information in an automated email which included the reason for his negative [REDACTED] as being the [REDACTED] complaint which was found against him.

- [REDACTED] contacted the complainant to outline to him how he can submit his Data Access Request and provide him with more information.

Thus, based on the information that was provided, the CNPD did not identify any infringement by the controller of the obligations set out in Regulation (EU) 2016/679 (GDPR) by [REDACTED].

As the complaint had only a limited personal impact, the CNPD has consulted the supervisory authority of Brandenburg (Germany) to determine whether the case could be closed. The CNPD and the supervisory authority of Brandenburg (Germany) agreed that, in view of the above, no further action was required and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 294755).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED], lodged with the supervisory authority of France (national reference 18022393) and submitted to the Luxembourg supervisory authority via IMI under Article 61 procedure 72561.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED”]), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope the complaint and assessment of the case

In the initial complaint on IMI, the complainant stated that he was a reviewer on the website [REDACTED] for a few years and that during those years, he published [REDACTED] reviews, usually with photos. Then, according to the complainant, [REDACTED] erased every single one of his reviews without letting him the time to retrieve them. He then contacted [REDACTED] in order to retrieve these reviews without success.

The complaint is thus based on Article 15 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) GDPR, in particular as regards the right of access of [REDACTED] to his personnel data processed by [REDACTED], mainly his reviews.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has informed the CNPD that it had investigated this matter and noted that the request sent by [REDACTED] on 4 September 2018 was not directed internally to the team responsible for processing DSARs and that for this reason, [REDACTED] was not informed of the actions taken for his request.

After having been contacted by the CNPD, [REDACTED] immediately escalated the complainant’s DSAR to the correct team and acted on the DSAR. [REDACTED] apologized for this human error and

confirmed to provide additional training to the relevant teams regarding the DSAR response process. It also assured that it took further steps to remind the internal departments on how to recognize a DSAR to ensure that they are routed to the correct team.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and the exercised right has been attended.

As the complaint had only a limited personal impact, the CNPD has consulted the supervisory authority of France to determine whether the case could be closed. The CNPD and the supervisory authority of France agreed that, in view of the above, the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 295819).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED] lodged with the supervisory authority of Germany, Bavaria, (national reference LDA-1085.3-10025/19-I) and submitted to the Luxembourg supervisory authority via IMI under Article 61 procedure 73786.

The complaint was lodged against the controller [REDACTED] (hereinafter “[REDACTED]”) which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

In the initial complaint on IMI, the complainant stated that further to his request to close his account and to erase the underlying personal data, [REDACTED] confirmed to have processed his request. The complainant however stated that his attempt to verify the actual closure of the account by logging into such account triggered [REDACTED] two-step verification procedure and that in this context he received a SMS from [REDACTED] containing a security code. In the light of the above, the complainant had doubts as to the actual closure of its account and erasure of the underlying personal data.

The complaint is thus based on Article 17.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) GDPR, in particular as regards the complainant’s request to erase his personal data and to explain why the two-step verification procedure was still in place for the complainant’s former account.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has confirmed that it had already initiated the complainant’s request for account closure and deletion. As a result, the customer account was not further accessible to the complainant, but unfortunately [REDACTED] have not yet been able to delete the phone number used for two-step verification for the complainant’s customer account due to a technical problem.

[REDACTED] informed the CNPD that as background, two-step verification adds an additional layer of security to the [REDACTED] customer account. Instead of simply entering the password when signing in to the [REDACTED] customer account, two-step verification requires the customer to enter a unique security code in addition to the password during sign-in. The customer can receive this security

code in a variety of ways depending on the option select during sign-up, including text message, voice call, or authenticator app. If a phone number is used, that number is associated with the customer account and kept for two-step verification purposes.

In the case of the complainant, [REDACTED] encountered a technical problem which prevented the phone number associated with the complainant's account from being deleted. This is the reason why the complainant still received the security code to his mobile phone when he tried to log in. However, [REDACTED] has immediately addressed this issue and have deleted the associated phone number.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and/or the exercised right has been attended.

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

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new and/or similar complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 295836).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED] lodged with the supervisory authority of Germany, Bavaria, (national reference LDA-1085.3-10571/19-I) and submitted to the Luxembourg supervisory authority via IMI under Article 61 procedure 92645.

The complaint was lodged against the controller [REDACTED]. (hereinafter “[REDACTED]”) which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

“The data subject states that upon request the deletion of their mobile phone was confirmed, however, the mobile number is still processed at [REDACTED].” Furthermore, it results from the complaint that [REDACTED] wished to connect his actual [REDACTED] account with said phone number which was previously associated with an already closed account.

The complaint is thus based on Articles 16 and 17 GDPR.

Based on said complaint, the CNPD requested [REDACTED] to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) GDPR, in particular as regards the erasure and/or rectification of the complainant’s phone data.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, [REDACTED] has confirmed that the closure request was completed and that the complainant should now be able to connect the phone number from the prior account to his current [REDACTED] account.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and the exercised right has been attended.

As the complaint had only a limited personal impact, the CNPD has consulted the supervisory authority of Bavaria (Germany) to determine whether the case could be closed. The CNPD and the supervisory authority of Bavaria (Germany) agreed that, in view of the above, no further action is required and that the cross-border complaint should be closed. Also, the complainant considered the case as resolved.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 295888).

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

For the National Data Protection Commission

Final decision

The present decision refers to the case/complaint of [REDACTED] lodged with the supervisory authority of Germany, Brandenburg, (national reference 136/18/1112) and submitted to the Luxembourg supervisory authority via IMI under Article 56 procedure 47964.

The complaint was lodged against the controller [REDACTED] (hereinafter "████████"), which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission ("CNPD") is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

The initial wording of the complaint on IMI stated that:

"The complainant requested access to data via E-Mail. Since no answer was received she called ██████ by phone. As an answer she was told that her identity has to be confirmed and that she will be prompted to send an id-card copy via e-mail in the near future. Since that E-Mail did not arrive, she tried to log-in to her account but was provided with safety-measures. A code was sent to her e-mail and she was prompted to verify that code via phone. She states that she did not save her phone number in the account by herself but that ██████ used the number she had used before to call ██████ the first time."

The complaint is thus based on Articles 5 and 15 of GDPR.

Based on said complaint, the CNPD requested ██████ to provide a detailed description of the issue relating to the complainant's data processing as per Article 58.1 a) GDPR, in particular as regards to her right of access as well as the origin and processing of her phone number.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the intervention by the Luxembourg supervisory authority, ██████ has confirmed to the CNPD that it received the complainants data access request on 1st June 2018. After confirming her identity, ██████ provided the information to her on 18th July 2018 and she acknowledged receipt of the information via e-mail on 24th July 2018 (*document provided to the CNPD*). Furthermore, the complainant did not provide any further details regarding what data she thinks ██████ has not provided to her.

With regard to the phone number (*known by the CNPD*), ██████ provided information to the CNPD which specified that the phone number was indeed provided by the data subject when the account was opened on 14 March 2018.

Thus, based on the information that was provided, the CNPD did not identify any infringement by the controller of the obligations set out in Regulation (EU) 2016/679 (GDPR) by [REDACTED].

As the complaint had only a limited personal impact, the CNPD has consulted the supervisory authority of Brandenburg (Germany) to determine whether the case could be closed. The CNPD and the supervisory authority of Brandenburg (Germany) agreed that, in view of the above, no further action or additional measures were needed and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 293852).

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

For the National Data Protection Commission



Deliberation No 19/RECL9/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.887 lodged against [REDACTED]

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 on the free movement of such data, and repealing Directive 95/46/EC (the 'GDPR');

Having regard to the Act of¹ August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime (hereinafter referred to as the 'Law of¹ August 2018');

Having regard to the Rules of Procedure of the National Commission for Data Protection adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the 'ROI');

Having regard to the complaints procedure before the National Commission for Data Protection adopted on 16 October 2020 (hereinafter referred to as the 'Complaint Procedure before the CNPD');

Having regard to the following:

I. Facts and procedure

1. In the framework of European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Lower Saxony (Germany) submitted to the National Data Protection Commission (hereinafter: "the CNPD") the complaint of [REDACTED] (national reference of the authority concerned: LFD 5.22-025-011-19/013) via IMI according to procedure Article 56-61808.
2. The complaint was lodged against the controller [REDACTED] which has its sole establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The initial claim in IMI stated the following:

*The complainant is bothered with unwanted fax advertisement by the controller [REDACTED]
[REDACTED] A written request of the complainant to stop sending direct Marketing
has been ignored by the controller.*

4. In essence, the complainant asks the CNPD to ask the controller to respect his right to object.

Deliberation No 19/RECL9/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.887 lodged against [REDACTED]

5. The complaint is therefore based on Article 21 GDPR.
6. On the basis of this complaint and pursuant to Article 57(1)(f) GDPR, the CNPD asked the controller to comment on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular as regards his right to object.
7. The controller provided the requested information within the time limits set by the CNPD.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, (...) if he considers that the processing of personal data concerning him or her constitutes a breach of this Regulation.*"
9. In accordance with Article 21(2) GDPR "*Where personal data are processed for marketing purposes, the data subject shall have the right to object at any time to the processing of personal data relating to him or her for such marketing purposes, including profiling insofar as it is linked to such a marketing*";
10. Article 56(1) GDPR states that "*the supervisory authority of the main establishment or single establishment of the controller or processor shall be competent to act as the lead supervisory authority in respect of the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60*";
11. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article by endeavouring to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange any relevant information*";
12. According to Article 60(3) GDPR, "*The lead supervisory authority shall, without delay, communicate 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 with a view to obtaining their opinion and shall take due account of their views*";

Deliberation No 19/RECL9/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.887 lodged against [REDACTED]

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- In fact, the complainant received unsolicited faxes, but they were addressed to another person (who could have been the former owner of the fax number),
- The personal data concerned was deleted without delay, preventing any other commercial messages.

3. Outcome of the case

14. The Plenary Training therefore considers that, following the investigation of this complaint, the controller has taken the appropriate steps to grant the complainant's request for a right of objection, in accordance with Article 21(2) of the General Data Protection Regulation.

15. Therefore, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted the supervisory authority of Lower Saxony (Germany) under Article 60(1) if it agreed to close the case. The Lower Saxony supervisory authority replied in the affirmative, with the result that the CNPD came to the conclusion that no further action was necessary and that the cross-border complaint could be closed.

In view of the above, the CNPD, sitting in plenary and deliberating unanimously, decided:

- Close complaint file No. 2.887 upon completion of its investigation, in accordance with the complaints procedure before the CNPD and after obtaining the agreement of the authority concerned.



Deliberation No 19/RECL9/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.887 lodged against [REDACTED]

Thus decided in Belvaux on 10 June 2022.

The National Commission for Data Protection

[REDACTED]
Chair

[REDACTED] Commissioner [REDACTED] Commissioner [REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



Deliberation No 20/RECL10/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 3.245 lodged against [REDACTED]

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of¹ August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime (hereinafter referred to as the ‘**Law of¹ August 2018**’);

Having regard to the Rules of Procedure of the National Commission for Data Protection adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROI**’);

Having regard to the complaints procedure before the National Commission for Data Protection adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Lower Saxony (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the authority concerned: LFD 5.22-025-011-18/051) via IMI according to procedure Article 56-53300.
2. The complaint was lodged against the controller [REDACTED] which has its sole establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The initial claim in IMI stated the following:



Deliberation No 20/RECL10/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 3.245 lodged against [REDACTED]

Since the year 2015 the complainant is bothered with unwanted fax advertisement by the controller [REDACTED]. Until now, repeated requests of the complainant to stop sending direct Marketing have been ignored by the controller. However, the complainant was not capable anymore to submit these requests.

4. In essence, the complainant asks the CNPD to ask the controller to respect his right to object.
5. The complaint is therefore based on Article 21 GDPR.
6. On the basis of this complaint and pursuant to Article 57(1)(f) GDPR, the CNPD asked the controller to comment on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular as regards his right to object.
7. The controller provided the requested information within the time limits set by the CNPD.

II. In law

1. Applicable legal provisions
8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, (...) if he considers that the processing of personal data concerning him or her constitutes a breach of this Regulation.*"
9. In accordance with Article 21(2) GDPR "*Where personal data are processed for marketing purposes, the data subject shall have the right to object at any time to the processing of personal data relating to him or her for such marketing purposes, including profiling insofar as it is linked to such a marketing*";
10. Article 56(1) GDPR states that "*the supervisory authority of the main establishment or single establishment of the controller or processor shall be competent to act as the lead supervisory authority in respect of the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60*";
11. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article by endeavouring*

Deliberation No 20/RECL10/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 3.245 lodged against [REDACTED]

to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange any relevant information;

12. According to Article 60(3) GDPR, "The lead supervisory authority shall, without delay, communicate 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 with a view to obtaining their opinion and shall take due account of their views'";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that the personal data concerned were deleted without delay.

3. Outcome of the case

14. The Plenary Training therefore considers that, following the investigation of this complaint, the controller has taken the appropriate steps to grant the complainant's request for a right of objection, in accordance with Article 21(2) of the General Data Protection Regulation.

15. Therefore, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted the supervisory authority of Lower Saxony (Germany) under Article 60(1) if it agreed to close the case. The Lower Saxony supervisory authority replied in the affirmative, with the result that the CNPD came to the conclusion that no further action was necessary and that the cross-border complaint could be closed.

In view of the above, the CNPD, sitting in plenary and deliberating unanimously, decided:



Deliberation No 20/RECL10/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 3.245 lodged against [REDACTED]

- To close complaint file No. 3.245 upon completion of its investigation, in accordance with the complaints procedure before the CNPD and after obtaining the agreement of the authority concerned.

Thus decided in Belvaux on 10 June 2022.

The National Commission for Data Protection

[REDACTED]
Chair

[REDACTED] Commissioner [REDACTED]

[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



Deliberation No 18/RECL8/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.882 lodged against [REDACTED]

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of¹ August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime (hereinafter referred to as the ‘**Law of¹ August 2018**’);

Having regard to the Rules of Procedure of the National Commission for Data Protection adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROI**’);

Having regard to the complaints procedure before the National Commission for Data Protection adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Austrian Supervisory Authority submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the authority concerned: D130.209) via IMI in accordance with Article 56-60144 procedure.
2. The complaint was lodged against the controller [REDACTED] which has its principal place of business in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The initial claim in IMI stated the following:
“Austrian complainant lodged complaint against respondent with main establishment in Luxembourg because there was no Reply to a request for Access within a month.
4. In essence, the complainant asked the CNPD to intervene with the controller to give access to the complainant’s data within one month.

Deliberation No 18/RECL8/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.882 lodged against [REDACTED]

5. The complaint is therefore based on Article 15 GDPR.
6. On the basis of this complaint and pursuant to Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, in particular as regards her right of access.
7. The controller provided the requested information within the time limits set by the CNPD.

II. In law

1. **Applicable legal provisions**
8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, (...) if he considers that the processing of personal data concerning him or her constitutes a breach of this Regulation.*"
9. In accordance with Article 15 GDPR "*The data subject shall have the right to obtain from the controller confirmation that personal data concerning him or her are being processed and, where such data are processed, access to such personal data and the following information (...).*"
10. Article 56(1) GDPR states that "*the supervisory authority of the main establishment or single establishment of the controller or processor shall be competent to act as the lead supervisory authority in respect of the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60*";
11. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article by endeavouring to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange any relevant information;*
12. According to Article 60(3) GDPR, "*The lead supervisory authority shall, without delay, communicate 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 with a view to obtaining their opinion and shall take due account of their views*".

Deliberation No 18/RECL8/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.882 lodged against [REDACTED]

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- [REDACTED] sent a letter requesting information under Article 15 GDPR, which was received on 7 November 2018 and the controller replied on 27 November 2018;
- [REDACTED] then sent additional questions, which she asked on 11 December 2018 and 31 January 2019. In response, the controller granted [REDACTED] access to her personal data by sending a document containing her personal data on 18 March 2019;
- On 29 March 2019, the email address recorded in [REDACTED]'s profile was deleted by the controller, as requested by the complainant. Confirmation of deletion was sent to the complainant on the same day;
- On 30 March 2019, [REDACTED] requested a further confirmation of the deletion of the same email address. On 9 April 2019, the controller confirmed the deletion of the corresponding email address by telephone and e-mail once again.
- The controller realised that this access to [REDACTED]'s personal data had actually been granted to her after the legal deadline, which was why [REDACTED] apologised. After internal investigation, it appears that this unexpected situation was caused by technical problems, combined with the end of the year rush and the holiday period at that time. Once the technical problem was detected and eliminated, access was granted and the document containing the personal data had been sent to [REDACTED]
- Finally, the controller drew the attention of its employees and business partners to the importance of this issue and to the fact that timelines are essential for processing customer access requests. Such a situation should therefore no longer be repeated.

3. Outcome of the case



Deliberation No 18/RECL8/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.882 lodged against [REDACTED]

14. The Plenary Training therefore considers that, following the investigation of this complaint, the controller has taken the appropriate steps to grant the complainant's request for access, in accordance with Article 15 of the General Data Protection Regulation.
15. Therefore, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
16. The CNPD then consulted the Austrian supervisory authority under Article 60(1) if it agreed to close the case. The Austrian supervisory authority replied in the affirmative, with the result that the CNPD came to the conclusion that no further action was necessary and that the cross-border complaint could be closed.

In view of the above, the CNPD, sitting in plenary and deliberating unanimously, decided:

- close complaint file No. 2.882 upon completion of its investigation, in accordance with the complaints procedure before the CNPD and after obtaining the agreement of the authority concerned.

Thus decided in Belvaux on 10 June 2022.

The National Commission for Data Protection

[REDACTED]
Chair

[REDACTED] Commissioner [REDACTED]



Deliberation No 18/RECL8/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 2.882 lodged against [REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



Deliberation No 23/RECL13/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.595 lodged against [REDACTED]

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of¹ August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime (hereinafter referred to as the ‘**Law of¹ August 2018**’);

Having regard to the Rules of Procedure of the National Commission for Data Protection adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROI**’);

Having regard to the complaints procedure before the National Commission for Data Protection adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the supervisory authority of Ireland submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the authority concerned: C-19-12-55) via IMI in accordance with the procedure Article 61-103737.
2. The complaint was lodged against the controller [REDACTED] which has its principal place of business in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The initial claim in IMI stated the following:

“The Irish data subject raised their initial concern to the DPC via webform received 29th November 2019. The DS outlines in their webform their concerns regarding the DC’s non

Deliberation No 23/RECL13/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.595 lodged against [REDACTED]

response to their erasure request which was sent 19th November 2019. The DS stated that they can still access their account and that [REDACTED] are still processing their request.

4. In essence, the claimant asks the CNPD to ask [REDACTED] to grant it access to its data, but without using the download tools in the [REDACTED] account.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and pursuant to Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular as regards his right to erasure.
7. The controller provided the requested information within the time limits set by the CNPD.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that “*without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, (...) if he considers that the processing of personal data concerning him or her constitutes a breach of this Regulation.*”
9. In accordance with Article 17 GDPR “*The data subject shall have the right to obtain from the controller the erasure, as soon as possible, of personal data concerning him or her and the controller shall have the obligation to erase such personal data as soon as possible, where one of the following grounds applies (...)*”;
10. Article 56(1) GDPR states that “*the supervisory authority of the main establishment or single establishment of the controller or processor shall be competent to act as the lead supervisory authority in respect of the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60*”;
11. According to Article 60(1) GDPR, “*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article by endeavouring to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange any relevant information;*

Deliberation No 23/RECL13/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.595 lodged against [REDACTED]

12. According to Article 60(3) GDPR, "The lead supervisory authority shall, without delay, communicate 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 with a view to obtaining their opinion and shall take due account of their views";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- [REDACTED] had in fact two [REDACTED] accounts associated with the same email address. From correspondence with [REDACTED], [REDACTED] understood that the second account was created by mistake by [REDACTED] and that it was a duplicate account. The main account was always open and was also actively used by [REDACTED] but, following a request from [REDACTED], the duplicate account was effectively closed.

[REDACTED] requested that the double account be deleted on 19 November 2019. An email was sent asking [REDACTED] to reply to the e-mail to confirm that he wanted to delete his account (as shown to the CNPD). [REDACTED] had no trace of [REDACTED] having responded to this email and confirming his request to delete the account, and [REDACTED]'s additional email suggested that he did not complete this step.

- On November 26, 2019, [REDACTED] sent another email stating that he could still access his account and asked to "delete the account" (as shown to the CNPD). This was accepted as evidence that [REDACTED] wanted to delete his account and that the [REDACTED] team started the process of deleting [REDACTED]'s duplicate account and closed the account on the same day. [REDACTED]'s customer service then informed [REDACTED] on November 26, 2019 (as shown to the CNPD).

3. Outcome of the case

14. The Plenary Training therefore considers that, following the investigation of this complaint, the controller has taken the appropriate steps to grant the request for the right of erasure of the complainant, in accordance with Article 17 of the General Data Protection Regulation.



Deliberation No 23/RECL13/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.595 lodged against [REDACTED]

15. Therefore, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted Ireland's supervisory authority under Article 60(1) if it agreed to close the case. The Irish supervisory authority replied in the affirmative, with the result that the CNPD came to the conclusion that no further action was necessary and that the cross-border complaint could be closed.

In view of the above, the CNPD, sitting in plenary and deliberating unanimously, decided:

- To close complaint file No. 4.595 upon completion of its investigation, in accordance with the complaints procedure before the CNPD and after obtaining the agreement of the authority concerned.

Thus decided in Belvaux on 10 June 2022.

The National Commission for Data Protection

[REDACTED]
Chair

[REDACTED]
Commissioner Commissioner



Deliberation No 23/RECL13/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.595 lodged against [REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Deliberation No 22/RECL12/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.130 lodged against [REDACTED]

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of¹ August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime (hereinafter referred to as the ‘**Law of¹ August 2018**’);

Having regard to the Rules of Procedure of the National Commission for Data Protection adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROI**’);

Having regard to the complaints procedure before the National Commission for Data Protection adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the authority concerned: Lda-1085.4-9559/18-I) via IMI in accordance with Article 56-61900 procedure.
2. The complaint was lodged against the controller [REDACTED] which has its principal place of business in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The initial claim in IMI stated the following:

The complainant submits that in a letter dated 30 August 2018 he applied to [REDACTED] for information pursuant to Art. 15 DS-GVO. Initially, this letter was not answered by the

Deliberation No 22/RECL12/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.130 lodged against [REDACTED]

company. Following a reminder dated 08.10.2018, the complainant received a standardised reply on 16.10.2018 in which the company referred to its website, in which the applicant could search for the desired information. The complainant looks this as a violation if information and the handing over of a copy of the data are discarded in this form.

4. In essence, the claimant asks the CNPD to ask [REDACTED] to grant it access to its data, but without using the download tools in the [REDACTED] account.
5. The complaint is therefore based on Article 15 GDPR.
6. On the basis of this complaint and pursuant to Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular as regards his right of access.
7. The controller provided the requested information within the time limits set by the CNPD.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that “without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, (...) if he considers that the processing of personal data concerning him or her constitutes a breach of this Regulation.”
9. In accordance with Article 15 GDPR “The data subject shall have the right to obtain from the controller confirmation that personal data concerning him or her are or are not being processed and, where such data are processed, access to such personal data and the following information (...);”
10. Article 56(1) GDPR states that “the supervisory authority of the main establishment or single establishment of the controller or processor shall be competent to act as the lead supervisory authority in respect of the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60”;

Deliberation No 22/RECL12/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.130 lodged against [REDACTED]

11. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article by endeavouring to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange any relevant information;*"
12. According to Article 60(3) GDPR, "*The lead supervisory authority shall, without delay, communicate 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 with a view to obtaining their opinion and shall take due account of their views'*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - [REDACTED] did not receive the first letter of August 2018, as it was not sent to the appropriate address of the data controller in Luxembourg (which is clearly stated in [REDACTED]'s privacy policy).
 - [REDACTED] received the reminder letter on 15 October 2018 and sent a reply on 16 October inviting him to use the download tools in the [REDACTED] account, as it is still the easiest way for the customer to identify and submit his request via the designated contact form.
 - [REDACTED] clearly reaffirms that if the customer does not wish, [REDACTED] will not deny other channels of access and use of other means of identification.
 - However, in this scenario, [REDACTED] must correctly identify the applicant as the respective customer account holder in order to ensure that personal data is disclosed only to the data subject.
 - On the basis of the letter received on 15 October 2018, [REDACTED] did not refuse the request for access to the data, but the controller was not able to correctly identify [REDACTED] on the basis of the information provided in the letter. [REDACTED] found only one customer account linked to the email address mentioned in the complainant's letter header and therefore sent an email on 16 October 2018 with detailed

Deliberation No 22/RECL12/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No 4.130 lodged against [REDACTED]

instructions on how to submit the access request via the designated contact form in its customer account.

- Subsequently, the controller had no further contact with [REDACTED] regarding the request for access.
- Following receipt of CNPD's letter concerning this claim, [REDACTED] again sent an email to the claimant asking it to confirm that it requested access to its data. [REDACTED] will then send the dataset to the complainant upon receipt of the complainant's affirmative reply.

3. Outcome of the case

14. The Plenary Training therefore considers that, following the investigation of this complaint, the controller has taken the appropriate steps to grant the request for the right of access of the complainant, in accordance with Article 15 of the General Data Protection Regulation.
15. Therefore, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
16. The CNPD then consulted the supervisory authority of Bavaria (Germany) under Article 60(1) if it agreed to close the case. The supervisory authority of Bavaria (Germany) replied in the affirmative, with the result that the CNPD came to the conclusion that no further action was necessary and that the cross-border complaint could be closed.

In view of the above, the CNPD, sitting in plenary and deliberating unanimously, decided:

- To close claim file No. 4.130 upon completion of its investigation, in accordance with the complaints procedure before the CNPD and after obtaining the agreement of the authority concerned.



**Deliberation No 22/RECL12/2022 of 10 June 2022 of the National
Commission for Data Protection sitting in plenary session on
complaint file No 4.130 lodged against [REDACTED]**

Thus decided in Belvaux on 10 June 2022.

The National Commission for Data Protection

[REDACTED]
Chair

[REDACTED] Commissioner [REDACTED] Commissioner [REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Deliberation No 21/RECL11/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No. 3.800 lodged against [REDACTED]

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of¹ August 2018 on the organisation of the National Commission for Data Protection and the General Data Protection Regime (hereinafter referred to as the ‘**Law of¹ August 2018**’);

Having regard to the Rules of Procedure of the National Commission for Data Protection adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROI**’);

Having regard to the complaints procedure before the National Commission for Data Protection adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the authority concerned: Lda-1085.3-4210/19-I) via IMI in accordance with Article 61-74310 procedure.
2. The complaint was lodged against the controller [REDACTED] which has its principal place of business in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The initial claim in IMI stated the following:

The complainant submits that he closed his [REDACTED] Account on 31.12.2018 and applied to [REDACTED] for the deletion of all data that is not subject to the statutory storage

**Deliberation No 21/RECL11/2022 of 10 June 2022 of the National
Commission for Data Protection sitting in plenary session on
complaint file No. 3.800 lodged against [REDACTED]
Sàrl**

regulations. The company has not complied with the request to delete the data despite several requests. On 07.02.2019, the complainant filed an application for information pursuant to Art. 15 DS-GVO. [REDACTED] then provided the complainant with an extract of the stored data and it turned out that wish lists, watch lists, dates of books read, marked text passages etc., which the complainant deleted long time ago, are still stored. [REDACTED] states, that they are going to store certain data due to various tax and legal storage obligations, but does not tell, which kind of data has to remain stored. The complainant understands this to mean that there is no real process for deleting the data.

4. In essence, the applicant asks the CNPD to:
 - ask [REDACTED] to delete all personal data related to its account,
 - to have access to the personal data that must be stored for specific legal, tax and accounting reasons after the account has been closed.
5. The complaint is therefore based on Articles 17 and 15 GDPR.
6. On the basis of this complaint and pursuant to Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, in particular as regards his right of erasure and his right of access.
7. The controller provided the requested information within the time limits set by the CNPD.

II. In law

1. **Applicable legal provisions**
8. Article 77 GDPR provides that “without prejudice to any other administrative or judicial remedy, any data subject shall have the right to lodge a complaint with a supervisory authority, (...) if he considers that the processing of personal data concerning him or her constitutes a breach of this Regulation.”
9. In accordance with Article 15 GDPR “The data subject shall have the right to obtain from the controller confirmation that personal data concerning him or her are or are not being processed and, where such data are processed, access to such personal data and the following information (...);”

Deliberation No 21/RECL11/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No. 3.800 lodged against [REDACTED]

10. In accordance with Article 17 GDPR “*The data subject shall have the right to obtain from the controller the erasure, as soon as possible, of personal data concerning him or her and the controller shall have the obligation to erase such personal data as soon as possible, where one of the following grounds applies (...)*”;
11. Article 56(1) GDPR states that “*the supervisory authority of the main establishment or single establishment of the controller or processor shall be competent to act as the lead supervisory authority in respect of the cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60*”;
12. According to Article 60(1) GDPR, “*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article by endeavouring to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange any relevant information*”;
13. According to Article 60(3) GDPR, “*The lead supervisory authority shall, without delay, communicate 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 with a view to obtaining their opinion and shall take due account of their views*”;

2. In the present case

14. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
 - The claimant requested the cancellation of his customer account on December 31, 2018 during a phone call with [REDACTED]’s customer service. The account was successfully closed and the claimant no longer had access to the account. Due to a human error, the customer service agent who processed the request did not follow all the steps required to disable the devices and delete the customer account. This error occurred in March 2019, when [REDACTED] responded to another request by the claimant to access his remaining data by providing him with a dataset including information from the claimant’s [REDACTED] device, such as read books and text passages marked with books that, under [REDACTED]’s policy, should have been deleted.

**Deliberation No 21/RECL11/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No. 3.800 lodged against [REDACTED]
[REDACTED]**

- Following a phone call with the complainant, [REDACTED] confirmed by e-mail on 5 March 2019 that the account had been closed and that [REDACTED] would ensure the deletion of the account. [REDACTED] also responded to the complainant's further investigation and explained that [REDACTED] should keep certain data such as booking documents concerning its previous orders for accounting purposes.
- [REDACTED] did not hear from the complainant after March 2019. In order to avoid any doubt, [REDACTED] again confirmed to the CNPD that the claimant's account data (including the above mentioned data elements relating to the claimant's [REDACTED] device) have been deleted (with the exception of the data retained for tax, legal and accounting reasons referred to above).
- For the sake of completeness, [REDACTED] again wrote to the complainant explaining in more detail what data is stored for specific legal, tax and accounting reasons.

3. Outcome of the case

15. The Plenary Training therefore considers that, following the investigation of this complaint, the controller has taken the appropriate steps to grant the request for the right to erasure and the request for the right of access of the complainant, in accordance with Articles 17 and 15 of the General Data Protection Regulation.
16. Therefore, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
17. The CNPD then consulted the supervisory authority of Bavaria (Germany) under Article 60(1) if it agreed to close the case. The supervisory authority of Bavaria (Germany) replied in the affirmative, with the result that the CNPD came to the conclusion that no further action was necessary and that the cross-border complaint could be closed.

In view of the above, the CNPD, sitting in plenary and deliberating unanimously, decided:

- Close Claim File No. 3.800 upon completion of its investigation, in accordance with the complaints procedure before the CNPD and after obtaining the agreement of the authority concerned.



Deliberation No 21/RECL11/2022 of 10 June 2022 of the National Commission for Data Protection sitting in plenary session on complaint file No. 3.800 lodged against [REDACTED]

Thus decided in Belvaux on 10 June 2022.

The National Commission for Data Protection

[REDACTED]
Chair

[REDACTED] Commissioner
[REDACTED] Commissioner

[REDACTED]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation No 23/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.264 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 171805**

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-10294/20-I) via IMI in accordance with Article 61 procedure - 171805.
2. The complaint was lodged against the controller [REDACTED], who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant alleges that the company makes it difficult or virtually impossible for him to delete his private customer account with various demands.

In addition to the private customer account, he also had a seller account. While he finally succeeded in deleting the seller account, the deletion of the private customer account was prevented by various inaccurate arguments.

**Deliberation No 23/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.264 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 171805**

For example, the termination of the private customer account is made dependent on a prior termination of the seller account, an allegedly existing outstanding debt that does not exist is cited, or it is said that the account has been hacked.

The complainant wishes assistance in enforcing his request for cancellation of his customer account.”

4. In essence, the complainant was stating that he encounters difficulties to obtain the closure of his [REDACTED] customer account and the deletion of his personal data linked with this account, as [REDACTED] informed him that there was an outstanding amount on his Amazon customer account preventing him to close the account, while – according to the claimant – there was no such outstanding amount. The complainant contacted [REDACTED] at several occasions to solve the issue, without any success at the date of the complaint. Thus, he asks the CNPD to request [REDACTED] to delete his [REDACTED] customer account and his personal data linked with this account.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that “*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*”
9. In accordance with Article 17 GDPR, the data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17 (1) GDPR

**Deliberation No 23/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.264 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 171805**

applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17 (3) GDPR.

10. Article 56(1) GDPR provides that “*(...) 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*”;
11. According to Article 60(1) 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*”;
12. According to Article 60(3) 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*”;

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:
 - The complainant had indeed a seller account and a customer account with [REDACTED].
 - For both accounts, [REDACTED] had already completed the complainant's request for account closure and data deletion of the personal information related to the accounts.
 - Regarding the complainant's seller account, the request for account closure and data deletion was processed the day that followed the request and the complainant was informed about it.
 - Regarding the complainant's customer account, the complainant experienced an issue to obtain the closure of the account, as an outstanding amount was existing in [REDACTED]'s systems.



**Deliberation No 23/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.264 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 171805**

- [REDACTED] confirmed that there was indeed an open amount for an older transaction regarding the complainant. However, [REDACTED] already completed the customer's request for account closure and data deletion at the date of the CNPD enquiry.
- The outstanding amount has thus been cleared and the complainant's request for account closure and data deletion has been completed. [REDACTED] also informed the complainant about this.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 GDPR.
15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
16. The CNPD then consulted the supervisory authority of Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.264 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority.

Belvaux, dated 27 March 2023

The National Data Protection Commission

Tine A. Larsen
Chair

Thierry Lallemand
Commissioner

Alain Herrmann
Commissioner

Marc Lemmer
Commissioner



**Deliberation No 23/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.264 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 171805**

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



**Deliberation No 24/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.342 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174271**

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-10738/20-I) via IMI in accordance with Article 61 procedure -174271.
2. The complaint was lodged against the controller [REDACTED], who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant states that since March 2020 she has been receiving parcels from [REDACTED] at regular intervals, all of which are sent from China.

She has contacted [REDACTED] and has repeatedly requested that all her accounts under her e-mail address be closed and her personal data deleted.

**Deliberation No 24/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.342 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174271**

On August 22, 2020, she received an e-mail from [REDACTED] confirming that the process of closing the account and deleting the data for all accounts under the e-mail address mentioned above had been initiated.

Although she was subsequently able to determine that her [REDACTED] account had been blocked/closed on 23/08/2020, she did not receive any confirmation that her personal data had actually been deleted. Rather, she has continued to receive unwanted parcel deliveries from China.

Furthermore, she filed a complaint against the company [REDACTED] that unknown third parties were apparently able to create customer accounts and place orders using her personal data, so that she was requested by debt collection companies to pay for ordered products which she had not ordered and whose order date was after the closure/blocking of her customer account.

Furthermore, she demands the deletion of all her personal data from [REDACTED] and the commissioned collection agency, as well as the renouncement of the debt collection."

4. In essence, the complainant asks the CNPD:
 - i. To request [REDACTED] to close all her accounts and delete her personal data registered with [REDACTED] as well as make [REDACTED] renounce to any debt collection.
 - ii. To check on the lawfulness of the processing.
5. The complaint is therefore based on Articles 17 and 5 (1) (f) GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by [REDACTED] and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to her request for erasure and the lawfulness of the processing in this particular case.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

**Deliberation No 24/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.342 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174271**

8. Article 77 GDPR provides that “*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*”
 9. In accordance with Article 5 (1) (f) of the GDPR “*Personal data shall be [...] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*”.
 10. In accordance with Article 17 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 (...)*”
 11. Article 56(1) GDPR provides that “*(...) 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*”;
 12. According to Article 60(1) 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*”;
 13. According to Article 60(3) 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*”;
- 2. In the present case**
14. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:

**Deliberation No 24/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.342 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174271**

- it completed the complainant's request for account closure and deletion of her personal data in connection with the accounts relating to the e-mail address (xxx) in August 2020;
- it investigated the case and informed the CNPD that [REDACTED] placed nine orders in April 2020 with the seller from China, which [REDACTED] had identified as the sender of the unwanted packages;
- that the seller's conduct in this case appeared to be a form of 'brushing', meaning that concretely in this case, the seller collected the complainant's address from her previous orders and then started using the address abusively to send unwanted packages (because in similar cases, the orders are initiated by sellers who would like to obtain positive ratings and references for their seller profile);
- according to [REDACTED]'s communication with [REDACTED] (i.e. [REDACTED] went back to the complainant to ask additional information regarding her request to block sellers from China following the letter from the CNPD), these orders were not debited from her bank account;
- [REDACTED] took further action after corresponding with the complainant in 2020, so that the accounts of the identified selling parts were permanently blocked and excluded from offering on [REDACTED];
- [REDACTED] inferred that following the letter by the CNPD, it was working on compiling the information on the sellers responsible for the unwanted packages and assured that once this was complete, it would share it with [REDACTED].;
- in addition, [REDACTED] confirmed that any bad debt on [REDACTED]'s account had been cleared so that there was no remaining financial damage and that [REDACTED] assured that in their announced communication with the complainant, [REDACTED] would provide clarification regarding the invoice.

3. Outcome of the case

15. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to demonstrate the lawfulness of the processing in accordance with Articles 5 and 6 GDPR and to grant the complainant's right to erasure of her personal data, in accordance with Article 17 GDPR.
16. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.



**Deliberation No 24/RECL11/2023 of 27 March 2023 of the
National Data Protection Commission, in a plenary session, on
complaint file No 6.342 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 174271**

17. The CNPD then consulted the supervisory authority of Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.342 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority.

Belvaux, dated 27 March 2023

The National Data Protection Commission

Tine A. Larsen
Chair

Thierry Lallemand
Commissioner

Alain Herrmann
Commissioner

Marc Lemmer
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



Deliberation No 22/RECL9/2023 of 27 March 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 5.865 lodged against the company [REDACTED] via IMI Article 56 procedure 153549

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of the Netherlands submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: Z2020-08067) via IMI in accordance with Article 56 procedure - 153549.
2. The complaint was lodged against the controller [REDACTED], who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“Complainant requested access to his personal data but did not receive any reply from the controller.”

4. In essence, the complainant asks the CNPD to request the controller to act on his access request.

5. The complaint is therefore based on Article 15 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to the lack of reaction by the controller to the complainant's access request.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 15 GDPR, "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information (...).*"
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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*";

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- The controller's records show that in May 2018, the complainant has indeed requested access to his personal data, but that at this time his request was unfortunately not processed.
- On January 18 2021 (after the CNPD's intervention), the controller has sent the requested information to the complainant, together with their apologies.
- Since 2018, the controller has improved and streamlined its process for handling GDPR requests. And pursuant to this particular complaint, it has further finetuned this process so as to avoid incidents like this one in the future.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right of access, in accordance with Article 15 of the GDPR.

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted the supervisory authority of the Netherlands, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of the Netherlands has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.



Deliberation No 22/RECL9/2023 of 27 March 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 5.865 lodged against the company [REDACTED] via IMI Article 56 procedure 153549

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 5.865 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 27 March 2023

The National Data Protection Commission

Tine A. Larsen
Chair

Thierry Lallemand
Commissioner

Alain Herrmann
Commissioner

Marc Lemmer
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.



Deliberation No 21/RECL8/2023 of 27 March 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 4.774 lodged against the company [REDACTED] via IMI Article 61 procedure 111847

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of France submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: 19022757) via IMI in accordance with Article 61 procedure - 111847.
2. The complaint was lodged against the controller [REDACTED], who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The data subject is the author of a book that she decided to withdraw from selling. She holds the full copyrights. She asked [REDACTED] to remove the webpage concerning the book, without success.”

**Deliberation No 21/RECL8/2023 of 27 March 2023 of the National
Data Protection Commission, in a plenary session, on
complaint file No 4.774 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 111847**

4. In essence, the complainant asks the CNPD to request [REDACTED] to act on her erasure request related to the reference pages of her book on [REDACTED]'s websites.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to the lack of reaction by the controller to the complainant's erasure request related to the reference page of her book..
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.*"
9. In accordance with Article 17 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 (...)*"
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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*

Deliberation No 21/RECL8/2023 of 27 March 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 4.774 lodged against the company [REDACTED] via IMI Article 61 procedure 111847

supervisory authorities concerned shall exchange all relevant information with each other";

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:
 - After further review, and noting that no copies were currently offered on [REDACTED], [REDACTED] voluntarily resolved [REDACTED]'s request by removing the detail page of her book from [REDACTED].
 - [REDACTED] provided to the CNPD the answer given to [REDACTED], as well as the previous correspondence exchanged with [REDACTED].

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right of erasure, in accordance with Article 17 of the GDPR.
15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.
16. The CNPD then consulted the supervisory authority of France, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of France has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.



Deliberation No 21/RECL8/2023 of 27 March 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 4.774 lodged against the company [REDACTED] via IMI Article 61 procedure 111847

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 4.774 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority(s).

Belvaux, dated 27 March 2023

The National Data Protection Commission

Tine A. Larsen
Chair

Thierry Lallemand
Commissioner

Alain Herrmann
Commissioner

Marc Lemmer
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation No 44/RECL17/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.648 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185283**

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-7692/20-I) via IMI in accordance with Article 61 procedure - 185283.
2. The complaint was lodged against the controller [REDACTED] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“The complainant states that he operated a business and was active as a seller on the [REDACTED] platform. His company no longer exists since 2014. On [REDACTED]’s platform, the company is still listed as a seller and the company refuses or is unable to delete this data. In the above-mentioned data record, he is named and published with his first and last name as a shareholder of the company, so that the scope of application of the GDPR is opened. He wishes the deletion of his personal data.”

4. In essence, the complainant asks the CNPD to delete his personal data relating to a former [REDACTED] seller account, which had been closed in 2014.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*";
9. In accordance with Article 17 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 (...)*";
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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*";

**Deliberation No 44/RECL17/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.648 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185283**

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:

- The account had indeed been closed and the imprint with the personal data has been removed from the website [REDACTED].
- [REDACTED] has deactivated the link and has deleted the complainant's data on [REDACTED]'s website.

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 of the GDPR.

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

16. The CNPD then consulted the supervisory authority Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

**Deliberation No 44/RECL17/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.648 lodged against the company [REDACTED]
via IMI Article 61 procedure 185283**

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- to close the complaint file 6.648 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 9 June 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

**Deliberation No 43/RECL16/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.647 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185234**

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 on the free movement of such data, and repealing Directive 95/46/EC (the ‘**GDPR**’);

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the ‘**Law of 1 August 2018**’);

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the ‘**ROP**’);

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the ‘**Complaint Procedure before the CNPD**’);

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) submitted to the National Data Protection Commission (hereinafter: “the CNPD”) the complaint of [REDACTED] (national reference of the concerned authority: LDA-1085.3-5614/20-I) via IMI in accordance with Article 61 procedure - 185234.
2. The complaint was lodged against the controller [REDACTED] (“[REDACTED]”) who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.
3. The original IMI claim stated the following:

“ Complainant wishes to delete his data. The company has not yet complied with the data erasure.”

4. In essence, the complainant asks the CNPD to request [REDACTED] to close his account and delete all his personal data.
5. The complaint is therefore based on Article 17 GDPR.
6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [REDACTED] to take a position on the facts reported by the complainant and in particular to provide a detailed description of the issue relating to the processing of the complainant's data, and in particular with regard to his right to erasure.
7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*";
9. In accordance with Article 17 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 (...)*";
10. Article 56(1) GDPR provides that "*(...) 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*";
11. According to Article 60(1) 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*";

12. According to Article 60(3) 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*";

2. In the present case

13. Following the intervention of the Luxembourg supervisory authority, [REDACTED] confirmed that:

- It received the complainant's request for account closure and data deletion on 10 April 2020 for the customer account related to his e-mail address.
- [REDACTED] informed the complainant on the same day that there was an open order which was about to be dispatched and that they would proceed with his request to close his account after the order was received.
- [REDACTED] subsequently confirmed to the complainant on 14 April 2020 that they were processing his request.
- [REDACTED] then completed the complainant's request to close his account later in the same month.
- However, when the complainant contacted [REDACTED] on 2 June 2020 requesting a confirmation that [REDACTED] had processed his request, he received a response from [REDACTED] stating that customer service had not received his recent message, and explaining other ways of contacting customer service. [REDACTED] understands that this lead the complainant to doubt if they had processed his initial request from April 2020 (which it did).

3. Outcome of the case

14. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure, in accordance with Article 17 of the GDPR.

15. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.



**Deliberation No 43/RECL16/2023 of 9 June 2023 of the National Data Protection Commission, in a plenary session, on complaint file No 6.647 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 185234**

16. The CNPD then consulted the supervisory authority Bavaria, pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded affirmatively, so that the CNPD has concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 6.647 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority.

Belvaux, dated 9 June 2023

The National Data Protection Commission

[REDACTED]
Chair

[REDACTED]
Commissioner

[REDACTED]
Commissioner

[REDACTED]
Commissioner

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.

Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. Reference is made to the complaint, lodged by [REDACTED] (the “complainant”) against [REDACTED] (the “controller”), referred to the Information and Data Protection Commissioner (the “Commissioner”) pursuant to article 61 of the General Data Protection Regulation¹ (the “Regulation”) by the Spanish supervisory authority (Agencia Española de Protección de Datos), acting as the concerned supervisory authority under the one-stop-shop mechanism.
2. The complainant alleged that the controller did not respond to a request to erase her personal data pursuant to article 17 of the Regulation (the “request”) within one month. The request was submitted by means of an e-mail dated the 13th August 2020 to the e-mail address [REDACTED]. The complainant argued that that this was the e-mail address which was made available on the controller’s privacy policy published on the official website.
3. In support of the allegations made, the complainant provided the Commissioner with a copy of the request and a document issued by the company [REDACTED] certifying that such e-mail was actually delivered to the controller.

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).

INVESTIGATION

4. Pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint together with the supporting documents.
5. On the 4th December 2020, the controller submitted the following principal legal arguments for the Commissioner to take into consideration during the legal analysis of the case:
 - i. that the complainant sent "*her erasure request on the 13 August 2020 to the email [REDACTED] which is an old email address of [REDACTED], and not the contact email for [REDACTED] entity and its customers support service as also displayed currently in [REDACTED] Spanish website*";
 - ii. the controller held that the correct e-mail address which should be used by the Spanish customers is [REDACTED] and in this regard, the controller provided a screen capture of an URL of its official website², where such e-mail address is visible;
 - iii. that the complainant submitted her request on an old e-mail address which is "*not monitored regularly by the [REDACTED] customer support agents*", and consequently, the controller held that the complainant's "*request didn't reach [REDACTED] DPO before 24th November 2020, after DPO received the complaint from IDPC and internal investigation was launched*";
 - iv. that the "*unfortunate incident of not replying within required deadline can be attributed to a degree of unintentional human error from the [REDACTED] side for not monitoring regularly the old mailbox and from [the complainant's] side for not addressing her request to the email address displayed validly on [REDACTED] webpage*";
 - v. that following an internal investigation conducted by the controller, it has been established that the incident was a fraud case, and "*the data and account related to [REDACTED] has been blacklisted and maintained in a way only being available to the [REDACTED]*

² [REDACTED]

police and judicial authorities and not being anymore subject to any further processing by [REDACTED] or any of its data processors”;

- vi. that the controller was obliged to retain the complainant's personal data for ten (10) years from the date of the closure of the complainant's account, and that such obligation emanates from “*Article 163 of the Companies Act, Cap. 386; articles 4(11) and 4(13) of the Cooperation with Other Jurisdictions on Tax Matters Regulations (S.L. 123.127); article 19 of the Income Tax Management Act, Cap. 372; articles 1964 and 1968 of the Spanish Civil Code; and the Maltese Prevention of Money Laundering and Funding of Terrorism Regulation (S.L. 373.01) article 13(2)*”;
- vii. that the controller held that, having “*finalised its internal investigation and reached the conclusion* [that the matter is a result of fraud], *the [REDACTED] will immediately contact [the complainant] to address her request, explain the reason for [REDACTED] being late with its reply and sincerely apologies for the late reply*”. The Commissioner requested the complainant to further substantiate its submissions with a copy of the letter sent to the complainant.

LEGAL ANALYSIS AND DECISION

- 6. Having examined article 12(3) of the Regulation, which stipulates that “*the controller shall provide information on the action taken on a request under Articles 15 to 22 to the data subjects without undue delay and in any event within one month of receipt of the request*” [emphasis has been added].
- 7. Having read article 12(3) of the Regulation in conjunction with article 17 of the Regulation, which disciplines the right of the data subject to erase his or her personal data undergoing processing under certain circumstances.
- 8. During the course of the investigation, the Commissioner established that the controller did not reply to the request submitted by the complainant to erase her personal data within the period stipulated by law.
- 9. In terms of article 17(1) of the Regulation, the “*data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay*

*and the controller shall have the obligation to erase personal data without undue delay” where one of the grounds listed in article 17(1)(a) to (f) applies. However, this rule is subject to a number of exceptions, in particular article 17(3)(b) which states that the right to erasure shall not apply “**for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject ...**” [emphasis has been added].*

10. Having observed recital 65 of the Regulation, which stipulates that “[a] data subject should have the right to have personal data concerning him or her rectified and a ‘right to be forgotten’ where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation” [emphasis has been added].
11. Whereas the Commissioner established that the processing of the complainant’s personal data is necessary for compliance with a legal obligation to which the controller is subject, and therefore the controller’s refusal to erase the complainant’s personal data is justified pursuant to article 17(3)(b) of the Regulation, the controller is still obliged to respond to the data subject request submitted by the applicant within the period stipulated by law.
12. In this context, the Commissioner examined the submissions provided on the 4th December 2020, whereby the controller stated that the e-mail address to which the complainant sent her request was not regularly monitored and consequently, this was replaced by a new e-mail address. Pursuant to article 24(1)³ of the Regulation and, as a general good practice, the controller shall implement the appropriate technical and organisational measures to ensure that data subject requests are addressed in a timely and appropriate manner.
13. Consequently, the Commissioner concluded that, by leaving an e-mail address unmonitored, the controller violated its duty of care under the law, and that this negligent behaviour hindered

³ “Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

the complainant from obtaining a response to a right of erasure request within the period stipulated by law.

14. As a consequence, the fact that the complainant did not obtain a response within the deadline stipulated by the law generated unnecessary prolonged uncertainty in relation to the lawfulness and transparency of the controller's data protection practices and operations.

On the basis of the foregoing, the Commissioner decides that the controller infringed:

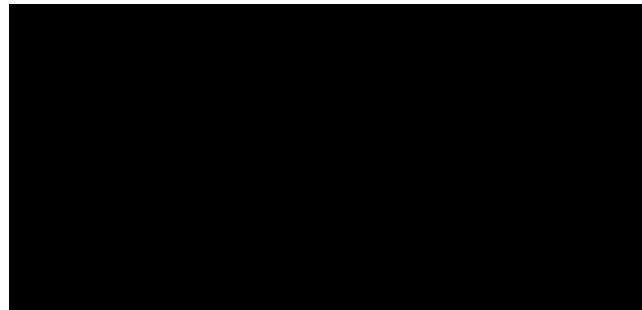
- i. article 12(3) of the Regulation when it failed to provide the complainant with information on the action taken on the request submitted on the 13th August 2020 to erase her personal data pursuant to article 17 of the Regulation; and
- ii. article 24(1) of the Regulation, for not having implemented the appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performed in accordance with the provisions of the Regulation, particularly, when it failed to set-up a mechanism to monitor incoming communications to the e-mail address [REDACTED]

By virtue of article 58(2)(b) of the Regulation, the controller is hereby being served with a reprimand and reminded that, in the event of a similar infringement, the Commissioner shall take the appropriate corrective action, as the case may be.

In terms of article 58(2)(d) of the Regulation, the Commissioner is instructing the controller to take the following corrective measures to bring its processing operations into compliance with the provisions of the Regulation by:

- i. setting-up a rule on the email account [REDACTED] so that the mailbox sends out automated responses to incoming e-mails informing the data subjects of the correct e-mail address; or
- ii. setting-up a rule whereby e-mails sent to the e-mail address [REDACTED] are automatically re-directed to the controller's correct e-mail address.

The controller shall provide the Commissioner with evidence of implementation of the aforementioned instructions within twenty (20) days from the date of receipt of this legally binding decision.



Decided today, the 27th day of April, 2021

Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. On the 4th June 2019, [REDACTED] (the “complainant”) lodged a complaint through his lawyer with the Personal Data Protection Office of Poland (the “Polish SA”) against [REDACTED] (the “controller” or the “bank”). The complainant contended that he has received two (2) requests dated the 25th May 2019 and the 28th May 2019, wherein the bank requested payment in relation to a loan agreement. The complainant strongly denied that he has ever concluded a loan agreement with the bank despite the requests for payment suggesting otherwise.
2. The complainant alleged that the bank has obtained his personal data from an unspecified source and consequently, his personal data has been used in an unauthorised manner. The complainant further added that a third-party probably has misused his personal data and this fact has indeed been reported to the Polish Police. For this reason, the complainant requested the Polish SA to determine the manner in which his personal data has come into the possession of the controller, including the basis and reason for which these were processed.
3. On the 30th January 2020, the Polish SA lodged a mutual assistance notification under article 61 of the General Data Protection Regulation² (the “Regulation”), wherein the Information and Data Protection Commissioner (the “Commissioner”) acted in its capacity of the lead supervisory authority in the light of the fact the controller’s main establishment is in Malta.

¹ [REDACTED]

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

4. As attachment to the above-mentioned notification, the Polish SA provided the Commissioner with a copy of the complaint. Subsequently, the Commissioner requested the Polish SA to provide additional correspondence, which the SA exchanged with the complainant's lawyer, including other related documentation. The Commissioner examined the letter sent by the complainant's lawyer to the bank³, dated the 4th June 2019, captioned the "loan agreement no. [REDACTED]" (the "**loan agreement**"), wherein the complainant referred to the request for payment dated the 28th May 2019, and:
 - a. instructed the bank to discontinue addressing any more letters or requests, and to desist from taking any action towards him in relation to the claims arising from the loan agreement, which the complainant said he has never signed;
 - b. informed the bank that the unlawful use of his personal data has been reported to the Police;
 - c. notified the bank that he did not consent to the processing of his personal data, and consequently, this matter has been referred to the Polish SA; and
 - d. informed the bank that in the event of non-observance of the above, the complainant may institute judicial proceedings.
5. On the 23rd July 2019, the Polish SA contacted the complainant's lawyer requesting him to rectify certain shortcomings identified in the complaint, dated the 4th June 2019.
6. On the 29th July 2019, the complainant's lawyer responded to the Polish SA's request by submitting the following arguments:
 - a. that the complainant has never concluded any contract with the bank, and therefore he did not entrust the bank with his personal data;
 - b. that the bank has been notified by the complainant that he did not agree with the processing of his personal data⁴, and that the bank did not reply to such communication;

³ The English version of the letter that was forwarded to the Commissioner by the Polish SA.

⁴ Supra, para. 4(a) to 4(d).

- c. that the Polish SA should have determined from which source the bank has obtained the complainant's data, considering that he has never entered into any loan agreements with it; and
- d. that the complainant was also expecting the Polish SA to order the erasure of his personal data undergoing processing by the controller.

INVESTIGATION

- 7. On the 9th March 2020, by virtue of article 58(1) of the Regulation, the Commissioner requested the controller to provide its submissions on the allegations raised by the complainant. In terms of this Office's internal investigation procedure, the Commissioner provided the controller with a copy of the complaint and the supporting documents attached thereto.
- 8. On the 24th March 2020, the controller submitted the following salient legal arguments:
 - a. that on the 13th June 2019, the controller "*received a notification letter from the District Police of Zywiec stating that [REDACTED] had submitted an application that his personal data had been used illegally and, as a consequence, a loan agreement was concluded with the Bank in his name but without his knowledge. On the same day, 13.06.2019, after receiving the above-mentioned notification letter from the Police, the Bank immediately stopped all debt collection activities relating to the Complainant and made a note in its systems accordingly. By this date, the Bank had still not received the letter sent on behalf of the Complainant*";
 - b. that on the 24th June 2019, the controller "*received a letter from [REDACTED] lawyer dated the 4th June 2019⁵ informing the Bank that [REDACTED] had not concluded a loan agreement with the Bank and that the relevant notification to Police had been submitted. Furthermore, the lawyer requested the Bank to discontinue addressing any more letters, requests or taking any other actions in relation to [REDACTED] on pain of action being taken against the Bank, in particular threatening the Bank with compensation claims*";

⁵ The letter was sent by post on the 6th June 2019.

- c. that the controller has never replied to the complainant's letter, dated the 4th June 2019, as it was the bank's understanding that "*as per action requested by representative, the Bank took notice in its systems to refrain from further contact with [REDACTED] and as regards personal data processing. As there was no request to reply to either [REDACTED] or his representative, the Bank refrained from such contact, also taking note the request of the lawyer in this respect, which seemed to indicate that correspondence from the Bank would be undesirable for his client*";
 - d. in relation to the source from which the personal data related to the complainant was collected, the controller provided that "*the loan application was submitted from IP address: [REDACTED] to the Bank's website [REDACTED] on 15.04.2019.*"
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].
9. On the 26th March 2020, the Commissioner referred to the statement made by the complainant's lawyer, specifically that the complainant "*does not consent to the processing of his personal data by you*", and requested the controller to put forward further submissions concerning the technical measures which the bank has implemented to ensure that the personal data linked with the complainant, were not subject to any further processing operations.
10. On the 3rd April 2020, the controller submitted the following considerations for the Commissioner to assess:
- a. "[a]s the complainant has requested to restrict the processing of his data, the Bank is not allowed to use his data, but we are permitted to store the personal data. In order to comply with the request, the Bank has extracted all the personal data linked to complainant's name [REDACTED]
[REDACTED] :

- b. the controller explained that “[t]he extracted data is then stored [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]”, and that “[t]he Bank-assigned client ID (this is not a personal identification number, but a number assigned to a customer when they are onboarded) and [REDACTED]
[REDACTED]; and
- c. the controller concluded that “[t]he Bank has security procedures in place to monitor the access and use of personal data in Bank’s systems. [REDACTED]
[REDACTED]
[REDACTED] *The principles of need-to-know and need-to-access as well as segregation of duties are enforced*”.
11. On the 24th April 2020, the Commissioner requested the controller to describe the clients’ onboard verification process, briefly referenced by the controller in its previous submissions⁶, and to provide copies of any relevant policies and procedures, which the controller had in place. Additionally, the Commissioner requested the controller to specify the legal basis upon which the complainant’s personal data was being retained, and the envisaged retention period thereof.
12. In response, on the 30th April 2020, the controller submitted a copy of the onboard identification and verification process adopted by the bank for customers located in Poland, and a copy of its “Credit Fraud Management Policy”.
13. The Commissioner sought to establish whether the bank has complied with the clients’ onboard verification process, at the time when the application for the loan in the name of the complainant was submitted. On the 22nd September 2020, the Commissioner requested the controller to produce the following documentation and information:

⁶ [REDACTED]
[REDACTED]

[REDACTED] Supra, para 8 (d).

- a. a copy of the loan application submitted by the applicant, in the name of the complainant;
 - b. a copy of the applicant's data, received by the controller by means of the bank payment;
 - c. a copy of the loan agreement signed by the applicant; and
 - d. the retention period established by the controller in connection with loan applications and agreements.
14. On the 28th September 2020, the controller submitted the requested documentation and information. In relation to the copy of the requested loan agreement signed by the applicant, the bank explained that, on the 15th April 2019, it sent to the complainant a copy of such agreement without the applicant's IBAN⁷, SECCI⁸ and other personal data and, following that, on the 16th April 2019, once the applicant's information was confirmed by means of receipt of a bank transfer⁹, the bank sent to the complainant an updated copy of the same loan agreement, including the information previously omitted. Accordingly, the controller provided the Commissioner with a copy of the two (2) versions of the loan agreement.
15. Additionally, the controller stated that “[t]he retention period for data related to loan's applications and agreements for the customers served in Poland is 10 years from the date when the account is closed”. In this regard, the controller explained that it has defined such retention period on the basis of the following:
- a. the IDPC and Malta Bankers' Association, Data Protection Guidelines for Banks (May 2018), according to which “*all account data is to be retained for a period often years from the date of closure of the respective account [...] subject to Article 163 of the Companies Act, Cap. 386; articles 4(11) and 4(13) of the Cooperation with Other Jurisdictions on Tax Matters Regulations (S.L. 123.127); and to article 19 of the Income Tax Management Act, Cap. 372*”. The controller pointed out that in the same guidelines, “*account data is defined as electronic data which relates to all aspects of*

⁷ International Bank Account Number.

⁸ Standard European Consumer Credit Information sheet.

⁹ Supra, footnote 5.

an account, excluding transaction data” and that “the information composed and gathered during the loan agreement signing process and concluded that most of the information and documentation is already composed and saved in electronic way, thus typically the Bank does not hold any information in paper format”. Therefore, the controller concluded that “both, account data and information should be retained for 10 years from the date of closure of the respective account”;

- b. the Polish Act on the Amendment to the Civil Code Act and certain other Acts of 13 April 2018¹⁰ (the “Act”). The controller explained that the Act amended the basic rules concerning limitation periods for civil law claims from 6 (six) to 10 (ten) years. The controller further provided that the Act applied to “*agreements in international transactions when the parties subject the agreement to Polish law or when according to Rome I regulations Polish law applied*”. On this point, the controller stressed that notwithstanding the fact that the loan agreement is governed by Maltese legislation, the consumer’s rights under Polish law are also applicable, as stipulated in article 26 of the loan agreement, and therefore, the duration of the retention period for account data and information has to be in line with the statutory deadline to bring proceedings against the bank under the applicable Polish law; and
- c. Regulation 13(2) of Prevention of Money Laundering and Funding or Terrorism Regulations (S.L. 373.01), which establishes “*a period of 5 years for retaining the documentation, data or information described in the same article 13(1) paragraph (a) as of the date the business relationship ends*”.

LEGAL ANALYSIS AND DECISION

16. For the purpose of this legal analysis, the Commissioner examined the initial complaint received by the Polish SA, including the additional correspondence¹¹ dated the 29th July 2019, and on the basis of this complaint, the Commissioner established that:
 - a. the complainant requested the controller to specify the source from which his personal data connected with the loan agreement has been obtained;

¹⁰ Polish Journal of Laws 2018, item 1104.

¹¹ The English version of the correspondence received by the Commissioner from the Polish SA.

- b. the complainant exercised his right to restriction of processing pursuant to article 18 of the Regulation, when he stated that he did not consent to the processing of his personal data by the controller;
- c. the complainant pointed out that he did not receive any response from the bank to its letter dated the 4th June 2019, by means of which, he exercised his right to restriction of processing, as mentioned above; and
- d. the complainant stated that he expected the Polish SA to order the erasure of his personal data processed by the controller.

Determining the source of the complainant's personal data

17. The Commissioner examined article 15(1)(g) of the Regulation, which stipulates that "*[t]he 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: [...] (g) where the personal data are not collected from the data subject, any available information as to their source*" [emphasis has been added].
18. Whereas the data subject has a right to obtain from the controller information in relation to the source from where his personal data has been collected, however such right is tied to the exercise of the right of access in terms of article 15 of the Regulation.
19. After examining the content of the letter dated the 4th June 2019, which the complainant sent to the controller, the Commissioner concluded that the complainant did not in any way exercise his right to access in terms of article 15 of the Regulation, and therefore, the controller was not legally obliged to provide the information concerning the processing within the period stipulated under article 12(3) of the Regulation.
20. Nonetheless, it should be remarked that, during the course of the investigation, the controller provided to the Commissioner information in relation to the source from where the complainant's personal data was obtained¹².

¹² Supra, para. 8(d).

The request to restrict the processing of personal data

21. The Commissioner examined article 4(3) of the Regulation, which defines “*restriction of processing*” as “*the marking of stored personal data with the aim of limiting their processing in the future*”.
22. Article 18 of the Regulation provides that the data subjects shall have the right to restrict the processing of their personal in certain circumstances. Accordingly, the Commissioner carefully examined article 18(1) of the Regulation, which stipulates that the “*data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: [...] (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead*”.
23. Furthermore, the Commissioner assessed article 18(2) of the Regulation, which explains the consequences triggered following a request to restriction filed by a data subject, wherein the restricted personal data “*shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State*”.
24. Recital 67 of the Regulation sheds further light on the methods of how the controller may restrict personal data, which may include, *inter alia*, “*temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website*”. Insofar as automated filing systems are concerned, the same recital establishes that “*restriction of processing should in principle be ensured by technical means in such a manner that the personal data are not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system*”.
25. In the letter dated the 4th June 2019, the complainant notified the controller that he did not consent to the processing of his personal data, and therefore, the complainant exercised a valid request in terms of article 18 of the Regulation, wherein he requested the controller to restrict the processing of his personal data after flagging the processing activity as unlawful.

26. During the course of the investigation, the Commissioner observed that the controller acknowledged that the complainant exercised his right to restriction of processing¹³ and in fact, the controller provided the Commissioner with information on the action taken to effectively comply with the complainant's request and restrict the processing of his personal data¹⁴.

The lack of response by the controller

27. Having assessed that article 12 of the Regulation ensures that substantive rights of data subjects, including the right to restrict processing, are safeguarded by establishing clear, proportionate and effective conditions as to how and when data subjects shall exercise these rights. In this regard, article 12 of the Regulation provides the modalities for the exercise of the data subjects' rights and establishes an obligation upon the controller to facilitate the exercise of these rights.
28. Accordingly, the Commissioner examined article 12(3) of the Regulation, which aims at ensuring the efficient exercise of data subjects' rights and binds the controller to "*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.*" This period may be extended to a maximum of three (3) months when the controller is handling a complex request in so far as the data subject has been informed about the reasons for such delay within one (1) month from the date of the original request.
29. From the contents of the documents provided by the complainant, including the submissions provided by the controller, the Commissioner concluded that the complainant's letter dated the 4th June 2019, by means of which, the complainant exercised his right to restriction of processing, was not responded to. The fact that the complainant's letter was never replied to, was in fact acknowledged by the controller in its submissions¹⁵.
30. The Commissioner analysed the reason provided by the controller for not responding to the complainant's letter and the related request to the right to restrict processing¹⁶. In this respect,

¹³ Supra, para. 10(a).

¹⁴ Supra, para. 10(b) and 10(c).

¹⁵ Supra, para 8(c).

¹⁶ Ibidem.

the controller alleged that a reply was not provided because “*there was no request to reply to either [REDACTED] or his representative [...] also taking note the request of the lawyer in this respect, which seemed to indicate that correspondence from the Bank would be undesirable for his client*”.

31. Having noted the statutory nature of the controller’s obligation derived from article 12(3) of the Regulation, and also taking into account that such obligation may not be waived in the event that the enquiring data subject does not include an explicit request to receive a response.
32. Having additionally established that the complainant’s lawyer instructed the bank to discontinue addressing to the complainant any more letters or requests or taking any action towards him **in relation to the claims arising from the loan agreement, and not in relation to the request to restrict processing, which is a right exercised by the complainant in terms of article 18 of the Regulation** [emphasis has been added].

The request to order the erasure of the personal data

33. In terms of article 17(1) of the Regulation, the “*data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*” where one of the grounds listed in article 17(1)(a) to (f) applies. This rule is subject to a number of exceptions, including article 17(3)(b) thereof which states that the right to erasure shall not apply “**for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject [...]**” [emphasis has been added].
34. Having observed recital 41 of the Regulation, which stipulates that “[w]here this Regulation refers to a legal basis or a legislative measure, **this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned. However, such a legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it, in accordance with the case-law of the Court of Justice of the European Union (the ‘Court of Justice’) and the European Court of Human Rights**” [emphasis has been added].

35. Having considered the European Data Protection Board's position¹⁷ in relation to article 17(3)(b) of the Regulation, according to which the notion of "unlawful processing" "*shall secondly be interpreted broadly, as the infringement of a legal provision other than the GDPR. Such interpretation must be conducted objectively by Supervisory Authorities, according to national laws or to a court decision*" [emphasis has been added].
36. Having given due regard to the information supplied by the controller during the course of the investigation concerning the retention period of the personal data processed within the context of loan applications and agreements¹⁸, and that the controller stated that the retention period is that of ten (10) years, starting from the date of the closing of the account. The controller also specified that such retention period was based on legal obligations to which it is subject deriving from Maltese law¹⁹.

On the basis of the foregoing, the Commissioner hereby decides that:

- a. **the complainant did not exercise his right to access pursuant to article 15 of the Regulation;**
- b. **by means of the letter dated the 4th June 2019, the complainant requested the controller to exercise his right to restriction of processing in terms of article 18 of the Regulation;**
- c. **the controller infringed article 12(3) of the Regulation when it failed to provide the complainant with information on the action taken on the aforesaid request within the period stipulated by law;**
- d. **the complainant's request to order the erasure of his personal data undergoing processing could not be met at the time of the issuance of this legally-binding decision, on the basis that the processing of the complainant's personal data is necessary for compliance with the legal obligations to which the controller is subject.**

¹⁷ European Data Protection Board, *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)*, Version 2.0, Adopted on 7 July 2020, para. 36, page 9.

¹⁸ Supra, para. 15.

¹⁹ Ibidem.

In terms of article 58(2)(b) of the Regulation, the controller is hereby being served with a reprimand and informed that in case of a similar infringement, the Commissioner shall take the appropriate corrective action, including the imposition of an administrative fine.

By virtue of article 26(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within twenty days from the service of the said decision as provided in article 23 thereof.

Decided today, the 2nd. day of September, 2021

Summary Final Decision Art 60

Complaint

EDPBI:MT:OSS:D:2021:272

Reprimand

Background information

Date of final decision:	02 September 2021
Date of broadcast:	02 September 2021
LSA:	MT
CSAs:	PL
Legal Reference(s):	Article 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject), Article 17 (Right to erasure), Article 18 (Right to restriction of processing)
Decision:	Reprimand
Key words:	Data source, Data retention, Data subject rights, Transparency, Restriction of processing, Legal obligation

Summary of the Decision

Origin of the case

On 4 June 2019 the Complainant lodged a complaint with the CSA alleging that the controller had obtained his personal data from an unspecified source and was requesting repayment of a loan which the complainant claimed he never took. He informed the CSA that he had been a victim of an identity theft by a third party, which he had reported to the police, and requested the CSA to determine how his data had come into the possession of the controller. The CSA transferred the complaint to the LSA on the 30th January 2020. Subsequently the LSA, after having requested additional information to the CSA, informed the controller of the complaint on 9 March 2020 and requested its submissions to the allegations of the complainant. The controller responded on 24 March 2020 stating that it had been informed by the police about the illegal use of the complaint's personal data and had immediately stopped all debt collection activities. The controller also had received a letter from the complainant requiring the former to refrain from processing any personal data of the complainant and to discontinue any communication with regard to the loan. The controller had decided not to reply to this letter based on the understanding that any further communication was undesirable for the complainant. As to the source from which the personal data had been collected, the controller explained that it had

been obtained through a loan application via the website after the applicant's identity had been verified. The LSA then started an investigation into the on-board verification process of the controller and requested additional documentation, which the controller submitted. The controller also informed the LSA that it was subject to legal obligations under which the retention period for personal data related to loan applications and agreements could go up to 10 years.

Findings

On the question of determining the source of the complainant's personal data, the LSA noted that despite the right available under Article 15(1)(g) GDPR, the complainant had not explicitly asked the controller to provide him with information regarding the source of his data. Nevertheless, the controller did provide this information to the LSA. As regards the request to restrict processing of the complainant's personal data, after carefully analysing Articles 18(1)(b) and (2) and Recital 67 GDPR, the LSA found that the controller acknowledged and complied with the complainant's request to restrict processing of his personal data. Regarding the lack of response by the controller to the complainant's letter requesting restriction of processing, the LSA noted that the controller was in violation of Article 12(3) GDPR which lays down an obligation to provide the complainant with information on the action taken on a request under Articles 15 to 22 GDPR without undue delay and in any event within one month of receipt of the request. As regards the request for erasure, the SA carefully considered Article 17(1) and (2) GDPR, Recital 41 GDPR and the EDPB Guidelines 5/2019 to decide that the data could not be deleted because processing was necessary to comply with legal obligations under the national law to which the controller is subject.

Decision

The controller was served with a reprimand in accordance with Article 58(2)(b) GDPR.

CDP/IMI/LSA/17/2020

Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. On the 28th May 2020, Mr [REDACTED] (the “complainant”) filed a complaint (the “complaint”) with the Spanish Agency for Data Protection (the “Spanish SA”) against [REDACTED]
¹ (the “controller”).
2. The complainant alleged that in October 2019, he had opened an account with the controller to carry out a few operations on the stock market, and that in December of the same year, he had requested the controller to close his account.
3. The complainant argued that, at the time of lodging the complaint, his account with the controller was still open, and he was still receiving messages from the controller. The complainant also contended that the controller had requested him to sign a copy of the agreement in order to close his account, due to the fact that such agreement had not been signed upon subscription.
4. Furthermore, the complainant maintained that, the day before the date of lodging the complaint, he had received a document from the controller’s external auditor (the “auditor”) wherein he was requested to confirm his balance at the end of the previous year and sign the document². The complainant held that in such document, not only his personal data were

¹ [REDACTED]

² Infra, para. 11.

shown, but also those of other customers, including postal addresses, names, surnames and account balances.

5. From the analysis of the supporting evidence attached to the case, more specifically the thread of e-mails exchanged between the complainant and the controller, it transpires that on the 23rd February 2020, the complainant requested the controller to unsubscribe him from e-mail notifications and close his account.
6. On the 24th May 2020, the controller replied to the complainant indicating the procedure to unsubscribe from e-mail notifications. On the same day, the complainant informed the controller about his intention to close his account and that he did not manage to do that by following the suggested procedure.
7. On the 26th May 2020, the controller informed the complainant that “[w]hen we checked our record we realized that you haven't signed the contract with [REDACTED]. Could you please access into your client portal by using below link and sign the agreement. [REDACTED]. Note : you should already receive an another email about your portal password. Kindly check your email box”.
8. On the same day, the complainant replied to the controller and stressed that, in spite of the fact that he had sent many e-mails requesting the controller to remove him from its systems, he was still receiving e-mails. The controller replied that “[a]fter you sign the agreement I will close your account and you won't receive any email no longer”.
9. On the 26th May 2020, the complainant rebutted that “I don't need to sign anything. I've been with you since September last year, and now you're asking me for I-don't-know-what-agreement. Furthermore, a workmate of yours already contacted me to process the cancellation, and told me that it was done, what means that it was not so. As per GDPR, when I request the removal and the withdrawal of [...] access to my data, you have to process it without signing any agreement”.
10. On the same day, the controller replied that “[...] This agreement should have been signed at the beginning of account opening process but you haven't signed this agreement. First of all

signing agreement is an obligation. It take five min signing then I will close your account and you will never receive any email from [REDACTED] [...].

11. On the 27th May 2020, the auditor wrote to the complainant requesting him to confirm his portfolio holdings and cash balances held by the controller on his behalf. When providing such information, the auditor attached, not only a copy of the complainant's balances, but also those pertaining to third parties.
12. On the 17th June 2020, the Spanish SA informed the Information and Data Protection Commissioner (the “**Commissioner**”) about the complaint by virtue of article 56 of the General Data Protection Regulation³ (the “**Regulation**”). The Commissioner decided to handle the case pursuant to article 56 of the Regulation and informed the Spanish SA accordingly. As a consequence, the Commissioner handled the complaint in terms of article 60 of the Regulation.

INVESTIGATION

13. On the 17th June 2020, pursuant to article 58(1) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant. In terms of this Office’s internal investigation procedure, the controller was provided with a copy of the complaint, together with the supporting documents attached thereto.
14. On the 20th June 2020, the controller responded to the Commissioner’s request, specifying that such submissions were about “*the complainant’s right of erasure request exercised by the complainant by virtue of the withdrawal of his consent to [REDACTED]’s access to the Personal Data*”. The controller presented the following principal legal arguments for the Commissioner to take into consideration during the legal analysis of the case:
 - i. that “*[REDACTED] is a company which performs investment services in accordance with its license as issued by the Malta Financial Services Authority (hereinafter referred to*

³ 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).

as the “MFSA”) under the Investment Services Act [Chapter 370 of the Laws of Malta] (hereinafter referred to as the “Act”). Accordingly, ■■■ is subject to a variety of obligations, including strict anti-money laundering and compliance related obligations, arising from, inter alia, the Act, subsidiary legislation as emanating therefrom, the Investment Services Rules for Investment Services Providers as issued by the MFSA, the Conduct of Business Rulebook which is likewise issued by the MFSA, the Prevention of Money Laundering Act [Chapter 373 of the Laws of Malta], the Prevention of Money Laundering and Funding of Terrorism Regulations [Subsidiary Legislation 373.01] and the Implementing Procedures issued by the Financial Intelligence Analysis Unit in terms of the provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations [S.L 373.01]. Furthermore, ■■■ is also regulated by numerous European regulations and directives”.

- ii. that “[o]ne such obligation to which ■■■ is subject is a yearly statutory audit conducted by an independent third party. This is a legal obligation to which ■■■ is subject and the processing of the Personal Data is necessary for compliance with such legal obligation”;
- iii. that “[t]herefore, whilst it is appreciated that any data subject may exercise the right to erasure of personal data in terms of Article 17(1) of the GDPR, Article 17(3) thereof provides exceptions to this right. Of relevance is Article 17(3)(b) which states that the right to erasure as set out in Article 17(1) of the GDPR shall not apply to the extent that processing thereof is necessary “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”;
- iv. that “[a]ccordingly, ■■■ did not fully erase the Personal Data by virtue of the fact that the processing thereof is required in order to comply with a legal obligation to which it is subject in accordance with Article 17(3)(b) of the GDPR”;

- v. that “[REDACTED] respectfully submits that despite the complainant’s request for erasure of the Personal Data, it had, and still has, every right and indeed, a legal obligation, to process the Personal Data in accordance with the provisions of the GDPR”;
 - vi. that “[...] the retention (for a certain time period) of such Personal Data forming the subject matter of the Complaint by [REDACTED] is further necessary in order for [REDACTED] to comply with its anti-money laundering obligations”;
 - vii. that in relation to the fact that the controller requested the complainant to sign an agreement, the controller provided that the agreement “was never signed at the beginning of the relationship between the complainant and [REDACTED] [...] is necessary in satisfaction of [REDACTED]’s legal obligations with respect to client onboarding procedures. The complainant was requested to sign this agreement prior to the opening of his trading account with [REDACTED] and has no relevance to his request for the erasure of the Personal Data”; and
 - viii. additionally, the controller contended that “without prejudice to the foregoing, it is recognized that in order for a controller of personal data to be obliged to delete personal data of a data subject following a request for such erasure in terms of the provisions of the GDPR, one of the grounds as set out in Article 17(1) thereof must apply, which is not the case in the matter at hand”.
15. On the 3rd September 2021, the Commissioner requested the following additional information from the controller:
- i. the legal basis for processing the complainant’s personal data;
 - ii. in the event that such legal basis is consent, evidence that the complainant has given consent for the processing of his personal data at the time when the business relationship commenced; and
 - iii. a copy of the controller’s policy/procedure related to the handling of the data subjects’ requests.

16. On the 7th September 2021, the controller submitted that “*the processing of the Claimant's personal data was therefore necessary for compliance with various legal obligations to which [REDACTED] is subject in accordance with Article 6(1)(c)*”. In support of its arguments, the controller attached a copy of its privacy policy, which copy was delivered to the complainant.
17. On the 9th September 2021, the Commissioner requested the controller to submit a copy of the controller's policy/procedure related to data subject's right of erasure requests, which the controller did not submit with its previous response.
18. On the 13th September 2021, the controller submitted a copy of its “Operations Department Manual Procedure” and of its “Compliance Manual”. The Commissioner noted that the procedure for handling the right of erasure requests was included in the first of the two documents.
19. On the 30th November 2021, the Commissioner requested the controller to provide any evidence to prove that the complainant's account was closed as requested by the complainant on the 23rd February 2020.
20. On the 30th November 2021, the controller confirmed that the last e-mail that was sent to the complainant was on the 26th May 2020. The controller reiterated that they “*explained him why we need this contract but he insisted to reject to sign the Contract and we Closed his account as of 26.05.2020 operations Department did not send another e-mail to the Client related with Account Closure*”. On the same day, as attachment to another email, the controller also provided “the screenshots of account closure”.

LEGAL ANALYSIS AND DECISION

21. As part of the investigation of this complaint, the Commissioner examined the part of the complaint, wherein the complainant contended that he had received a document, which contains the personal data of third parties. In terms of article 77(1) of the Regulation, a complaint may only be lodged with a supervisory authority if the data subject considers that the processing of personal data relating to him or her infringes the provisions of the Regulation. It therefore follows that the complainant was not one of the affected data subjects, and therefore, for the purposes of this legal analysis, this part of the complaint is being

dismissed. Having said this, the Commissioner reserve the right to start a separe investigation on the alleged personal data breach committed by the controller's auditor.

22. In this regard, in terms of article 57(1)(f) of the Regulation, the Commissioner proceeded to examine, to the extent appropriate, the subject-matter of the complaint, specifically : (i) the complainant's request to exercise his right to erasure; and the (ii) timing of the request.

The complainant's request to exercise the right to erasure

23. Having noted that the protection of natural persons in relation to the processing of their personal data is a fundamental right recognised by article 8(1) of the Charter of Fundamental Rights of the European Union⁴. Within this context, the rights of the data subjects as laid down in articles 12 to 22 of the Regulation are the fulcrum and the basis of the law, and their role is crucial to ensure the effective and comprehensive protection of their personal data processed by controllers.
24. Having examined the right to erasure as laid down in article 17 of the Regulation, according to which the data subject shall have the right to obtain from the controller erasure of his personal data and the controller shall have the obligation to erase personal data without undue delay. The exercise of the right to erasure is subject to the applicability of one of the legal grounds listed in paragraph 1 thereof.
25. Having noted that, by way of exemption from the general rule, article 17(3) of the Regulation, which prescribes that paragraphs 1 and 2 shall not apply insofar as the processing is necessary for certain, specific purposes or compelling requirements, as exhaustively provided therein.
26. Having given due regard to the fact that, in this respect, article 17(3)(b) of the Regulation excludes the applicability of the right to erasure to the extent that processing is necessary 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.

⁴ Charter of Fundamental Rights of The European Union, 2012/C 326/02.

27. Having examined the controller's submissions, wherein the latter declared that it was subject to legal obligations mandating that certain customer records – which include personal data – are retained for a stipulated period of time⁵. In this respect, the controller declared that "*the retention (for a certain time period) of such Personal Data forming the subject matter of the Complaint by [REDACTED] is further necessary in order for [REDACTED] to comply with its anti-money laundering obligations*".
28. Having observed that for the purpose of the Prevention of Money Laundering and Funding of Terrorism Regulations, Subsidiary Legislation 373.01, the controller is deemed to be a subject person. Article 13(2) of S.L. 373.01 stipulates that certain documentation, data or information as referred to in sub-regulation 1 thereof, shall be retained for a period of five (5) years commencing from the triggering events prescribed therein.
29. Having further determined that indeed, processing of customers' records by the controller is necessary for compliance with the aforesaid provision, to which the controller is subject.
30. Having considered that, as declared by the controller⁶, the complainant's account has been closed on the 26th May 2020, and thus, the five-year period prescribed by the aforesaid provision had not elapsed at the time when the complainant lodged his complaint in terms of article 77(1) of the Regulation.
31. In view of the foregoing, the Commissioner concludes that, at the time when the complaint was lodged, the grounds listed in article 17(1) of the Regulation did not apply to the extent that processing is necessary for compliance with a legal obligation to which the controller is subject, and which requires processing by virtue of regulation 13(2) of S.L. 373.01.

The timing of the request

32. Having examined article 12 of the Regulation, which establishes clear, proportionate and effective conditions as to how and when data subjects shall exercise their rights provided by the Regulation.

⁵ Supra, para. 14(1).

⁶ Supra, para. 20.

33. Having noted paragraph 3 thereof, which aims at ensuring the efficient and timely exercise of data subjects' rights binding the controller to "*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*" [emphasis has been added].
34. Having considered that on the 23rd February 2020, the complainant requested the controller to exercise his right to erasure pursuant to article 17 of the Regulation and that in response, the controller requested the complainant to sign and return the subscription agreement. In addition, the controller informed the complainant on how to unsubscribe from receiving e-mail notifications.
35. In the correspondence exchanged between the controller and the complainant, the Commissioner could observe that the controller failed to inform the complainant about the steps taken in relation to the right to erasure request, and instead requested the complainant to sign and return the subscription agreement. The Commissioner emphasises that any failure on the controller's part to fulfil its own procedural or legal obligations, in this specific case to ensure that the complainant signs the subscription agreement, shall be independent of, and certainly shall not have an impact on, the exercise of the complainant's data protection rights.
36. Having further examined that the controller's procedure⁷ concerning the right of erasure requests, included in the "*Operations Department Manual*" submitted to this Office, wherein it resulted that the controller did not follow such procedure whilst handling the right to erasure request exercised by the complainant.
37. Having considered the Guidelines issued by the Article 29 Working Party, which provide that "[...] ***failure to read and abide by existing policies, human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner, failure to adopt policies (rather than simply failure to apply them) may be indicative of negligence***"⁸

⁷ "[t]he 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. [...] If the request of the Client is related with erasure of Personal Identification Document(s), [REDACTED] informs the Client that his request is not possible as per related rules and regulations and said documents will be kept at least 5 years in our records [...]" [emphasis has been added].

⁸ Article 29 Data Protection Working Party, *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*, 17/EN WP 253, page 12.

[emphasis has been added]. In this regard, the Commissioner established that, despite the fact that the controller had in place a policy in relation to the handling of the right to erasure requests, however, it failed to comply with its own procedure, which is an indicator of the fact that the controller acted negligently when the request submitted by the complainant was not handled in a timely manner, as prescribed in article 12(3) of the Regulation.

On the basis of the foregoing, the Commissioner hereby decides that the controller infringed article 12(3) of the Regulation, when it failed to provide the complainant with information on the action taken in relation to his right to erasure request submitted on the 23rd February 2020, within one (1) month of receipt of such request.

By virtue of article 58(2)(b) of the Regulation, the controller is being served with a reprimand and is informed that in case of another similar infringement, the Commissioner shall take the appropriate corrective action, including the imposition of an administrative fine.

In terms of article 58(2)(d) of the Regulation, the controller is hereby being ordered to provide the complainant with a reply to his right of erasure request and his request to close his account. This order shall be implemented with ten (10) days from the date of receipt of this legally-binding decision and the controller is requested to inform the Commissioner with the action taken to comply with such order immediately thereafter.

The controller is additionally being reminded that, by virtue of article 12(1) of the Regulation, the reply to the complainant shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular by including information relating to the specific legislation which obliges the controller to comply with the requirements deriving therefrom and retain personal data for the prescribed timeframe.



Information and Data Protection Commissioner

Decided today, the 28th day of February, 2022

Information and Data Protection Commissioner

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. On the 30th October 2020, Mr [REDACTED] (the “complainant”) lodged a complaint with the Berlin Commissioner for Data Protection and Freedom of Information (the “Berlin SA”) against [REDACTED], trading as [REDACTED] (the “controller”).
2. The Berlin SA lodged a mutual assistance notification under article 61 of the General Data Protection Regulation² (the “Regulation”), wherein the Information and Data Protection Commissioner (the “Commissioner”) acted in its capacity as the lead supervisory authority. In this context, the Berlin SA forwarded to the Commissioner a translated copy of the initial complaint and of the evidence attached thereto.
3. From the analysis of the documentation received, it transpires that, on the 22nd September 2020, the complainant exercised the right to access his personal data with the controller in terms of article 15 of the Regulation. On the same day, the controller responded to the complainant requesting him to submit a certified copy of his identity card or passport.

¹ [REDACTED]
[REDACTED]
[REDACTED]

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

4. On the 22nd September 2020, the complainant provided the controller with a photo of his identity card and held that in his views there were no grounds for requesting a certified copy of the document.
5. In subsequent e-mail exchanges between the controller and the complainant, the controller sustained that a certified copy of the complainant's identity card was necessary for identity verification purposes, considering that the complainant's request involved the transmission of sensitive data. On the other hand, the complainant observed that, according to him, the request for a certified copy of his identity card for identity verification purposes was unlawful and ran contrary to the Regulation. The complainant further added that, for the purpose of confirming his identity, the controller should have used other information in its possession, such as his e-mail address.

INVESTIGATION

6. On the 28th January 2021, pursuant to article 58(1) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant. Within this context, the Commissioner requested the controller to submit (i) a copy of the policy to identify and verify the identity of subscribers; (ii) reference to any legal basis to require additional information /documents to confirm subscriber's identity; and (iii) any specific reason why the complainant was requested to provide further information / documents to confirm his identity. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint together with the supporting documents attacted thereto.
7. By means of an e-mail dated the 2nd February 2021, the controller submitted the following principal legal arguments for the Commissioner to take into consideration during the legal analysis of the case:
 - i. that the controller receives "*several false requests from fraudsters trying to get users data*" by "*trying to mimic our players email address, or their close relatives to use our client's emails*", thus the controller needs to adopt additional measures to verify players' authenticity, including requesting proof of identity;

- ii. that “[o]ccasionally or in case our customer support agents are not fully satisfied, we do request additional method of verification, that is a certified or notarized copy” of users’ identification documents, and this was defined in recital 64 of the Regulation as ”*identity verification*“;
 - iii. that the last communication with the complainant was on the 30th October 2020, when the complainant “*was advised by a customer support agent that his request would be escalated to the relevant department and the request was forwarded 9to Floor Manager*”;
 - iv. that “[a]ccording to [the controller’s] procedures the case remains open for 30 days and if the request is not processed further it closes as “*Case Closed - Player did not provide required ID within 30 days*”;
 - v. that ”*the data subject [has] multiple accounts with us, we do require that his identity be verified to process his GDPR request*”; and
- the controller provided a copy of the procedure “*Managing Personal Data Requests Procedure*” dated the 30th April 2020 and approved by the company CEO, a file entitled “*Examples of fraudulent cases*” and copy of a Power Point presentation entitled “*GDPR Guidelines and Processes*”.
8. On the 2nd February 2021, with reference to the controller’s claim that the complainant had multiple accounts with the controller, the Commissioner requested the controller to specify: (i) why having multiple accounts was considered a valid reason to require additional proof of identity; (ii) whether all the complainant’s accounts were under the online casino ██████████ or with other casinos operated by the controller; (iii) whether the complainant filed the right of access request for all his accounts or for a specific account; and (iv) whether the e-mail address from which the controller received the right of access request was the same e-mail address that the complainant used to register his account on the online casino(s) or otherwise.

9. On the 4th February 2021, the controller informed the Commissioner, that “[l]ooking further to the [complainant’s] account we have found that this player had only one account with us”. The controller further added that “our support agents before sending any personal info they need to ensure that the request is legit. Technically there are always ways to false the senders email address and or a relative or friend get access to that email account. This happened a few times and fortunately because we follow our procedures we did not let this happen”.
10. On the same day, following the receipt of the above-mentioned email, the Commissioner requested the controller to provide additional clarifications to verify: (i) whether the procedure “Managing Personal Data Requests” submitted earlier on was adhered to, and (ii) whether it requested the complainant to confirm his e-mail address pursuant to the “Template - GDPR Identity Verification” and the “Template - GDPR Identity confirmed”³. The Commissioner also instructed the controller to submit copies of any documents where users were informed that a certified copy of their identity document may be requested by the controller as additional proof of identity.
11. On the same day, the controller replied that “customer support agents are there to assist our clients [...] based on the user request and attitude we need to ensure that the person we are dealing on the other side is the actual person. As a company we prefer to follow our processes and even waste more recourses that we need just to ensure the security and privacy of our customers”.
12. By means of an email dated the 9th February 2021, the Commissioner reiterated his requests for the controller to provide evidence of adherence to the procedure “Managing Personal Data Requests” and to confirm that the complaint’s e-mail address was requested pursuant to the “Template - GDPR Identity Verification” and to the “Template - GDPR Identity confirmed”.
13. On the 10th February 2021, the controller further provided that “[t]he verification procedure was followed by our agent. The player email address was validated and recorded as per internal process. [...] Personal data needs to be protected, and we had to ensure confidentiality, integrity and availability above all. Any data subject-access requests made by

³ The Commissioner received these documents from the controller during the course of the investigation of a separate case.

unauthorized persons will result in a breach. This is what we want to avoid in these type of cases". The controller also submitted a copy of their Privacy Policy and stressed that "[w]e do not specify in our Privacy Policy the type of ID verification we require in order to process a GDPR request".

LEGAL ANALYSIS AND DECISION

14. For the purpose of this legal analysis, the Commissioner sought in essence, to establish whether, by requesting the complainant a certified copy of his identity document prior to complying with his data subject's request submitted pursuant to article 15 of the Regulation, the controller has complied with its obligation to facilitate the exercise of data subject rights vis-à-vis article 12(2) of the Regulation.
15. By examining article 12(2) of the Regulation, the Commissioner has noted that such provision aims at ensuring that substantive rights of data subjects are safeguarded by establishing clear, proportionate and effective conditions as to how and when data subjects shall exercise their fundamental rights. The same article stipulates that "*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*" [emphasis has been added].
16. Furthermore, recital 64 of the Regulation states that 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[...]*" [emphasis has been added].
17. Having noted that, although the Regulation does not prescribe how to authenticate a data subject, in one of its guidelines⁴, the Article 29 Working Party ("WP29") has shed some light on the measures that a controller may adopt to verify the identity of the requesting party.
18. The WP29 elaborates that, where a data subject provides additional information enabling his or her identification, the controller shall not refuse to act on the request. Moreover, the WP29 articulates its position in the sense that "*[i]n essence, the ability for the data controller to request additional information to assess one's identity cannot lead to excessive demands and*

⁴ Article 29 Working Party, *Guidelines on the right to data portability*, 16/EN, WP 242 rev.01.

to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested” [emphasis has been added].

19. Having further assessed that whilst the Regulation does not define the “*reasonable measures*” which may be used by the controller to verify the identity of the requesting person, recital 57 of the Regulation exemplifies a reasonable measure in the context of online services and online identifiers. In this regard, recital 57 states that verification may occur, “*for example through authentication mechanism such as the same credentials, used by the data subject to log-in to the on-line service offered by the data controller*“ [emphasis has been added].
20. In this connection, the controller’s request to verify the identity of the data subject shall be proportionate and, unless strictly necessary, the controller shall not require a broader range of personal data other than that which has already been processed prior to the request.
21. The Commissioner stresses that when the controller processes “*additional information*” for the purpose of identity verification, the controller shall ensure that such processing activity complies with the data minimisation principle pursuant to article 5(1)(c) of the Regulation. In this regard, the requested data shall be adequate, relevant and limited to what is necessary in relation to the purpose of the processing, in this case consisting in the identification of the data subject.
22. In this context, it is relevant to observe that the controller should take into account the broad range of categories of personal data included in a copy of an identity document and the risk arising from the processing of such personal data.
23. After examining the submissions, including the documents and clarifications provided by the controller, the Commissioner noted that the controller’s procedure for ID verification does not dictate that a certified copy of the identity document is requested in every case, **but only in rare cases, where the customer support representative has doubts about the data subject’s authenticity.** Additionally, such documents contain no references to requests concerning certified copies of identity documents for verification purposes upon receipt of a data subject request.

24. Initially, the controller explained that such doubts originated from the fact that the complainant had multiple accounts with the controller. However, at a later stage, the controller informed the Commissioner that the complainant had only one account.
25. Furthermore, the controller held that the request for a certified copy of an identity document following a data subject's request, was justified due to certain cases that the controller had previously suffered, whereby data subjects' requests were fraudulently submitted by third parties on behalf of, or acting as, the account holders. Nonetheless, the Commissioner assessed that such a fraudulent attempt has not occurred in the case under examination, given that the complainant's request was submitted by the same account holder.
26. In the present case, the Commissioner is of the view that the controller had no reason to have doubts concerning the complainant's identity, especially after the controller confirmed that the complainant had only one account. In any event, the controller could have used other reasonable measures to verify his identity, which means are as equally effective and efficient.
27. It therefore follows that the controller could have used measures which include *inter alia*, matching the information and personal data provided by the complainant with the identity document on file and, or requesting confirmation of further details, such as biographical details and details concerning the complainant's activity or usage of the controller's platforms.
28. As a consequence of the unjustified request for a certified copy of the complainant's identity card for identity verification purposes, the controller has not facilitated the exercise of the right of access by the complainant.

On the basis of the foregoing, the Commissioner hereby decides that the controller infringed article 12(2) of the Regulation for not having facilitated the exercise of the right of the complainant pursuant to article 15 of the Regulation.

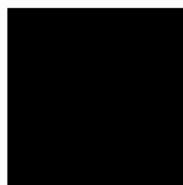
In terms of article 58(2)(b) of the Regulation, the controller is hereby served with a reprimand and informed that in case of a similar infringement, the Commissioner shall take the appropriate corrective action, including an administrative fine.

In terms of article 58(2)(d) of the Regulation, the Commissioner is hereby ordering the controller to respond to the right of access request filed under article 15 of the Regulation by providing the complainant with a copy of his personal data undergoing processing by virtue of article 15(3) of the Regulation, as well as any other relevant information in terms of Article 15(1) thereof, letters (a) to (h).

The controller shall comply with the above order within five (5) days from the date of receipt of this legally binding-decision and inform the Commissioner immediately thereafter.

In terms of article 83(6) of the Regulation, non-compliance with the aforesaid order shall “*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*”.

By virtue of article 26(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), any person to whom a legally binding decision of the Commissioner is addressed, shall have the right to appeal in writing to the Information and Data Protection Appeals Tribunal within twenty days from the service of the said decision as provided in article 23 thereof.



Information and Data Protection Commissioner


Decided today, the *4th* day of March, 2022

Information and Data Protection Commissioner

CDP/IMI/LSA/20/2021

vs

COMPLAINT

1. On the 18th December 2020, [REDACTED] (the “complainant” or the “data subject”) lodged a complaint with the Supervisory Authority of Spain (Agencia Española de Protección de Datos, hereinafter the “Spanish SA”) pursuant to article 77(1) of the General Data Protection Regulation¹ (the “Regulation”) against [REDACTED] [REDACTED] (the “controller”).

2. In his complaint, that data subject argued that:
 - a. the controller, together with other entities based in Spain, entered his data into the [REDACTED] insolvency register³ (“[REDACTED”]), in spite of the fact that he had not given his authorisation to the controller to disclose his data to third parties at the time of signing the contract with the controller⁴, nor at any later stage;

 - b. the controller never informed him that he could have been included in an insolvency register, and about the insolvency registers that the controller participated in;

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.

² [REDACTED] is a private limited company registered under the laws of Malta with registration number [REDACTED] and having registered address at [REDACTED]

³ The [REDACTED] insolvency register is owned and managed by [REDACTED] [REDACTED] company incorporated under the laws of Spain with registration number [REDACTED] and having registered address at [REDACTED].

⁴ On the 13th March 2020, the complainant concluded a repayment agreement with the controller.

- c. the controller did not include him in the [REDACTED] register in a faithful manner, so that he could exercise his rights as soon as he was entitled to;
 - d. on the 26th November 2020, he exercised his right to erasure with [REDACTED]. According to the complainant, the controller and the other entities which included his data in the [REDACTED] register failed to effectively erase his personal data without substantiating the reason for not doing so; and
 - e. that the amount of the debts is inaccurate.
3. In support of his complaint, the data subject submitted:
- a. a copy of an extract from the [REDACTED] registry dated the 27th November 2020, wherein an entry of the 7th June 2019 made by the controller shows a debt owed by the complainant to the controller;
 - b. a copy of a second extract from the [REDACTED] registry dated the 9th December 2020, wherein an entry of the 8th May 2019 made by the controller shows another debt owed by the complainant to the controller; and
 - c. a copy of the reply of [REDACTED] of the 9th December 2020 to the complainant's request to erase his personal data filed on the 26th November 2020, wherein [REDACTED] informed the complainant that it would not erase the data entered in the register by the controller given that the latter confirmed its correctness.
4. By virtue of article 56 of the Regulation, the Spanish SA identified the Information and Data Protection Commissioner (the "**Commissioner**") as the lead supervisory authority competent to handle the complaint. The Commissioner confirmed with the Spanish SA that it is indeed the lead supervisory authority for the present case, and he proceeded to investigate the complaint on the basis of the procedure set out in article 60 of the Regulation.

INVESTIGATION

5. On the 5th February 2021, pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the

complainant. In terms of this Office’s internal investigation procedure, the controller was provided with a copy of the complaint together with the supporting documents attacted thereto.

6. By means of an e-mail dated the 22nd February 2021, the controller submitted the following principal legal arguments for the Commissioner to consider in the legal analysis of the case:

- i. that the data subject was in a portfolio that the controller purchased from [REDACTED] ([REDACTED]);
- ii. that on the 8th August 2018⁵, the complainant was made aware of the purchase of his debt by means of a “welcome letter” (the “**welcome letter**”), wherein he was informed about the possibility that his data could be notified to insolvency files, or credit bureaus. According to the controller, it is not necessary to obtain the data subject’s consent to be reported to [REDACTED], but it is sufficient to inform him or her correctly. The controller attached a copy of this letter;
- iii. that on the 26th March 2019, the controller sent to the complainant another written payment request whereby he was informed of the possibility that his details could be notified to insolvency, or credit bureau files. The controller attached a copy of this letter;
- iv. that on the 7th May 2019, given that he had not paid the outstanding debt, the complainant was registered in [REDACTED] by the controller;
- v. that on the 26th November 2020, the complainant exercised his right to erasure directly with [REDACTED], which request was refused because his debt was pending and the requirements for registering him into the register were met; and
- vi. that on the 2nd February 2021, he was removed from [REDACTED] because legal proceedings were initiated in relation to the debt owed.

7. On the 4th November 2021, the Commissioner requested the controller to provide him with evidence that the welcome letter was delivered to the complainant.

⁵ This letter is dated the 11th August 2018.

8. On the 9th November 2021, the controller submitted a certification issued by its service provider in charge of dispatching outbound mail which, in the controller's opinion, demonstrates that the letter of the 11th August 2018 was sent to the complainant and that it was not returned.
9. On the 9th November 2021, the Commissioner requested the controller to confirm the delivery method of the letter, i.e. regular or registered mail.
10. On the 16th November 2021, the controller confirmed that the document was not sent by registered letter, which means that the controller does not have any written confirmation, or acknowledgement of delivery. The controller pointed out that local regulations do not require that such communication is sent by registered letter. In addition, the controller sustained that in subsequent telephone calls between the controller and the complainant, the latter acknowledged receipt of the welcome letter.
11. On the 15th February 2022, the Commissioner requested the controller to specify the legal basis pursuant to which the personal data were transferred by the controller to [REDACTED].
12. On the 18th February 2022, the controller responded that “[t]he legal basis for reporting these data to [REDACTED] is legitimate interest art. (6.1.f GDPR) of the creditor but and also public interest (art. 6.1.e GDPR), as Credit Bureaus help to preventing excessive indebtedness from growing in our country (gives information to financial entities/banks about someone who is asking for a loan and it contributes to the stability of financial system) and prevent excessive burden for the economy. Also, this data communication to Credit Bureaus is provided in article 20 of the Spanish Data protection Law (Spanish GDPR transposition Law) as a lawful and legitimate data processing”.
13. On the 21st March 2022, the Commissioner requested the controller to specify the date when the controller received the complainant's personal data from [REDACTED]. The controller responded by means of an email dated 28th March 2022, wherein it stated that the complainant's personal data was received for the first time on the 31st July 2018, which is the date when a debt portfolio purchase agreement between [REDACTED] and the controller was signed before a notary in Spain.
14. On the 30th March 2022, the Commissioner further requested the controller to submit a copy of such agreement.

15. On the 1st April 2022, the controller submitted a notarial testimony stating that a purchase of a debt portfolio occurred on the 31st July 2018, including an informal translation into English. However it did not submit a copy of the debt portfolio purchase agreement as requested by the Commissioner. Hence, on the 22nd April 2022, the Commissioner reiterated his request.
16. On the 27th April 2022, the controller submitted a copy of a “purchase and assignment portfolio without recourse deed”, dated the 31st July 2018, entered into between the legal representatives of [REDACTED] and the controller.

LEGAL ANALYSIS AND DECISION

17. In the legal analysis of the case, the Commissioner sought to examine and determine whether:
 - i. the controller complied with its obligations in terms of transparency in respect of the complainant when the controller received the complainant’s personal data from [REDACTED]; and
 - ii. the controller processed the complainant’s personal data in a lawful manner when it disclosed them to [REDACTED].

The obligation to provide information to the data subject

18. Transparency is a long-established feature of the law of the EU⁶ and one of the key principles of processing personal data. Together with the principle of lawfulness and fairness, it is enshrined in article 5(1)(a) of the Regulation, which provides that personal data shall be “*processed lawfully, fairly and in a transparent manner in relation to the data subject*” [emphasis added].
19. One of the components of the transparency obligation is the provision of information to data subjects relating to fair processing⁷ in the manner prescribed by law. The Regulation set forth the categories of information that shall be provided to a data subject in relation to the processing of their personal data, more specifically, by virtue of article 13 thereof, when the data is

⁶ Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679, WP 260 rev. 01, as last revised and adopted on the 11th April 2018 (“WP 260”), page 4.

⁷ Ibid.

collected from the data subject, and by virtue of article 14, when the data is obtained from another source⁸.

20. In the welcome letter, the controller declared that it had obtained the complainant's personal data from [REDACTED], which means that article 14 of the Regulation applies to the present case.
21. Article 14 of the Regulation places an obligation upon the controller to provide the data subject with details about the processing activity where the personal data have not been obtained directly from him or her, including:
 - (a) the identity and the contact details of the controller and, where applicable, of the 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 basis for the processing;
 - (d) the categories of personal data concerned;
 - (e) the recipients or categories of recipients of the personal data, if any;
 - (f) where applicable, that the controller intends to transfer personal data to a recipient in 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 to obtain a copy of them or where they have been made available.
22. Paragraph 2 thereof stipulates that in addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

⁸ WP 260, page 13.

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
 - (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
 - (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (e) the right to lodge a complaint with a supervisory authority;
 - (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
 - (g) 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.
23. Paragraph 3 of article 14 of the Regulation regulates the timeframes within which the required information shall be provided to the data subject. As clarified by the Article 29 Working Party⁹, the general rule is that the information shall be provided to the data subject by no later than one (1) month after having obtained the personal data.
24. In the present case, the controller obtained the complainant's personal data after it had purchased a debt which the complainant owed to [REDACTED]. The Commissioner therefore proceeded to read the "purchase and assignment portfolio without recourse deed" dated the 31st July 2018¹⁰ and particularly recital III thereof, which states that, on the 10th July 2018, the

⁹ WP 260, pages 15 and 16.

¹⁰ Supra, para. 18.

controller filed a binding offer with [REDACTED] for the portfolio of unpaid credit rights that included the debt owed by the complainant to [REDACTED]. In the same recital, the parties acknowledged that the controller was given the opportunity to audit certain documentation related to the same portfolio.

25. Given that the portfolio included the debt owed by the complainant to [REDACTED], as confirmed by the controller in its submissions¹¹, this fact unequivocally implies that the controller had obtained the complainant's personal data on, or before, the 10th July 2018, which is the date when the controller made a binding offer with [REDACTED] to purchase the debt portfolio.
26. The controller should have therefore provided the complainant with the information of article 14 of the Regulation at the latest by the 10th August 2018.
27. Notwithstanding this, the controller only provided such information to the complainant on, or after the 20th August 2018¹², which is the day when the welcome letter was dispatched to the complainant by controller's service provider in charge, and which is more than one (1) month from the date of obtaining the complainant's personal data.
28. Pursuant to article 14(1)(e) of the Regulation, the controller shall inform the data subject about the recipients or categories of recipients of the personal data, if any. Whilst the complainant argued that the controller had neither informed him that he could have been included in an insolvency register, nor about the controller's participation in the insolvency registers, through the welcome letter, the controller specified that in case of further insolvency, his personal data could have been communicated by [REDACTED] to any entity responsible for insolvency registers or credit bureaus.

The lawfulness of the processing

29. At the outset, the Commissioner observed the principle of lawfulness of processing as held in article 5(1)(a) of the Regulation, pursuant to which, each and every data processing operation shall have a lawful ground for processing. Article 6(1) thereof stipulates what may constitute

¹¹ Supra, para 6(i).

¹² Supra, para. 8. In its declaration, the service provided stated that the welcome letter was generated, printed and transferred to the outbound mailing service on the 20th August 2018.

such a legal basis, taking also into consideration all the other core principles for processing personal data as set out in article 5 of the Regulation.

30. During the course of the investigation, the controller submitted that the processing was necessary for the purposes of the legitimate interests pursued by both the controller and third parties. In this regard, the controller sought to protect the following interests: (a) to pursue debt collection; (b) to inform the public, including financial entities and banks, about the complainant's indebtedness, which contributes to the stability of the financial system.
31. In this regard, the Commissioner assessed article 6(1)(f) of the Regulation, which provides that the processing shall be lawful if it "*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 [...]*" [emphasis added].
32. The Commissioner interprets "*interest*" to be the broader stake that a controller may have in the processing, or the benefit that the controller or third parties may derive from such processing.
33. By virtue of the principle of accountability, it is for the controller to make its own assessment on a case-by-case basis in order to determine whether the interest is legitimate and therefore fulfills the requirements of article 6(1)(f) of the Regulation.
34. The Commissioner therefore examined the interest invoked by the controller for processing the complainant's personal data when it transferred such personal data to the insolvency register. Having given due regard to the clarity and specificity of the identified interest, being the aim of pursuing debt collection on the one hand, and ensuring that third parties can make accurate assessments when making lending decisions on the other hand, the Commissioner established that the interest at stake is indeed legitimate.
35. At the same time, having duly examined the circumstances of the case, the Commissioner established that there are no indicia that such interest is overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

On the basis of the foregoing considerations, the Commissioner hereby decides that the controller infringed article 14(3) of the Regulation for not having provided the complainant with the information set forth in article 14(1) and 14(2) of the Regulation within one (1) month from obtaining his personal data from [REDACTED].

By virtue of article 58(2)(b) of the Regulation, the controller is hereby brought served with a reprimand. In case of further similar infringements, the Commissioner shall take the appropriate corrective action, which may include the imposition of an effective, proportionate and dissuasive administrative fine.

On the other hand, the Commissioner hereby decides that the controller complied with its obligation to provide the complainant with information pursuant to the requirement set forth in article 14(1)(e) of the Regulation by means of its letter dated the 11th August 2018, and that the controller processed the complainant's personal data in a lawful manner when it transferred such personal data to [REDACTED], given that the processing was necessary for the purposes of the legitimate interest pursued by the controller, and that such interest was not overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

In terms of article 78 of the Regulation as further implemented under Part VII of the Data Protection Act (CAP. 586 of the laws of Malta), any party to this decision shall have the right to an effective judicial remedy by filing an appeal in writing before the Information and Data Protection Appeal Tribunal within 20 days from the service of this decision¹³.



(Signature) Date: 2022.06.08 [REDACTED]



Information and Data Protection Commissioner

Decided today, the 8th day of June, 2022

¹³ More information about the Tribunal and the appeals procedure is accessible on our office's portal at <https://idpc.org.mt/appeals-tribunal/>

Information and Data Protection Commissioner

CDP/IMI/LSA/19/2022

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. On the 11th June 2020, [REDACTED] (the “complainant”) lodged a complaint (the “complaint”) with the supervisory authority of Denmark (Datatilsynet, hereinafter the “Danish SA”) against [REDACTED]¹ (the “controller”) pursuant to article 77(1) of the General Data Protection Regulation² (the “Regulation”).
2. By virtue of article 56 of the Regulation, the Danish SA identified the Information and Data Protection Commissioner (the “Commissioner”) as the lead supervisory authority competent for the handling of the complaint. The Commissioner confirmed with the Danish SA that it is indeed the lead supervisory authority and proceeded to investigate the complaint on the basis of the procedure set out in article 60 of the Regulation.

INVESTIGATION

3. On the 11th June 2020, the complainant filed a complaint with the Danish SA and submitted the following principal arguments:

¹ [REDACTED] is a private limited company incorporated in Malta and operating in the online gaming sector with registration number [REDACTED] and registered address at [REDACTED].

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

- a. that “[REDACTED] seems to store more data than what is necessary – even though I have used my right to be forgotten. They have even confirmed completing the deletion process. They have sent me a file containing all the data that is still in their systems after this process was completed”;
 - b. that “I wonder a lot about the amount of data, as I don’t understand that they can lawfully store so much data regarding me. When I contracted them about it, they said that it was necessary to store the data due to legal obligations”;
 - c. that “I full understand that [REDACTED] has to store some data in order to document some things to the [REDACTED] authorities. I cannot understand thought that they lawfully can store that much data, and I want it to stop as far as my assumption is correct”;
 - d. that the controller satisfied his request to have his personal data erased. He noted that “these data are what they have regarding me after responding to my request to be forgotten. It is my clear impression that they do not have a legal basis for keeping all these data when I have requested deletion”.
4. In this regard, the controller submitted its reply to rebut the arguments made by the complainant and highlighted the following salient points:
- a. that the controller is a group of undertakings with its main establishment located in Malta and although the controller operates in Denmark under a Danish license, its website which is only available to the Danish market is operated by the main establishment, namely [REDACTED], a company incorporated under the laws of Malta, which is the controller responsible for the data processing through such platform;
 - b. that the complainant closed his account on the 2nd May 2020, and exercised his right to be forgotten on the 4th May 2020, and the controller replied to the request on the 18th May 2020;
 - c. that when a customer exercises such right, no further processing takes place in relation to the individual, apart from the retention of personal data which is either required to

comply with legal obligations or to establish, exercise or defend legal claims which may be instituted against the controller;

- d. that the controller emphasised that as a licensed operator, it is subject to obligations stemming from [REDACTED] regulatory and licencing requirements, notably those relating to [REDACTED];
- e. that the controller is also a subject person in terms of Directive EU 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (commonly known as the 4th Anti-Money Laundering Directive) as transposed under the Laws of Malta, and therefore the controller noted that such law imposes an obligation upon the controller to retain documentation concerning business relationship with a customer or after the date of an occasional transaction;
- f. that it is evident that the controller “*is unable to fully exercise the complainant’s request as this would hinder our compliance with legal obligations to which we are subject as well as our legitimate rights at law. In this regard, it is respectfully being submitted that most of the personal data relating to the complainant is indeed still necessary within the meaning of Article 17(1)(a) of the GDPR*”;
- g. that the controller referred to the retention periods and criteria used to establish such time frames, which information is made available on the controller’s website³; and
- h. that upon signing-up to use the controller’s services, a customer must accept the ‘*Terms & Conditions*’ and confirm that the privacy policy has been read and consequently, all the information contained in the privacy policy including the retention periods applicable to the processing of personal data have been duly made available to the complainant, in compliance with the transparency principle under the Regulation.

LEGAL ANALYSIS

- 5. The Commissioner proceeded to carefully examine the privacy policy available on the website of the controller, which must be accepted by the customer prior to signing-up to use its services.

³ [REDACTED]

The privacy policy which sets out general information in relation to the controller's retention periods, particularly that for anti-money laundering purposes, states that the controller has a legal obligation to keep its customer's personal data up to ten (10) years from the closure of the account.

6. In terms of article 17(1) of the Regulation, the “*data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay*” where one of the grounds listed in article 17(1)(a) to (f) applies. However, this rule is subject to a number of exceptions, in particular article 17(3)(b) which states that the right to erasure shall not apply “**for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject ...**” [emphasis has been added].
7. In this regard, the controller is subject to legal obligations which require processing of personal data even following the termination of the customer relationship. In terms of regulation 13 of the Prevention of Money Laundering and Funding of Terrorism Regulations, Subsidiary Legislation 373.01, the controller shall retain documents and information for a period of five (5) years which “*may be further extended, up to a maximum retention period of ten years, where, after a thorough assessment of the necessity and proportionality of such further extension, it is concluded that the extension is justified as necessary for the purposes of the prevention, detection, analysis and investigation of money laundering or funding of terrorism activities by the Financial Intelligence Analysis Unit, relevant supervisory authorities or law enforcement agencies*” [emphasis has been added].
8. In accordance with the definition of processing as held in article 4(2) of the Regulation, processing “*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*” [emphasis has been added]. This definition demonstrates that the retention of personal data constitutes processing of personal data, therefore the controller shall continue to comply with the requirements and principles until the destruction of the personal data as required by law.

On the basis of the foregoing, the Commissioner concludes that the right to erasure is not absolute, and it does not apply if the processing is necessary for compliance with a legal obligation to which the controller is subject. In such case, the Commissioner concludes that the controller did not infringe article 17 of the Regulation and, consequently the complaint is hereby being dismissed in its entirety.

In terms of article 78 of the Regulation, as further implemented under Part VII of the Data Protection Act (CAP. 586 of the laws of Malta), any party to this decision shall have the right to an effective judicial remedy by filing an appeal in writing before the Information and Data Protection Appeal Tribunal within twenty (20) days from the service of this decision⁴.

[Redacted]
Digitally signed
by [Redacted]

(Signature) Date: 2022.06.28
10:16:37 +02'00'

[Redacted]
Information and Data Protection Commissioner

⁴ More information about the Tribunal and the appeals procedure is accessible at <https://idpc.org.mt/appeals-tribunal/>

Information and Data Protection Commissioner

CDP/IMI/LSA/01/2021

[REDACTED]
vs
[REDACTED]

COMPLAINT

1. On the 15th November 2020, [REDACTED] (the “complainant”) lodged a complaint (the “complaint”) with the supervisory authority of Austria (Österreichische Datenschutzbehörde, the “Austrian SA”) against [REDACTED].¹ (the “controller” or “[REDACTED]”) pursuant to article 77(1) of the General Data Protection Regulation² (the “Regulation”).
2. By virtue of article 56 of the Regulation, the Austrian SA identified the Information and Data Protection Commissioner (the “Commissioner”) as the lead supervisory authority competent for the handling of the complaint. The Commissioner confirmed that it is indeed the lead supervisory authority and proceeded to investigate the complaint on the basis of the procedure set out in article 60 of the Regulation.
3. In his complaint, [REDACTED] alleged that the controller had forwarded his personal data to another [REDACTED], [REDACTED]³ (“[REDACTED”]), which consequently, used this information to defend itself in judicial proceedings instituted by the complainant against [REDACTED] before the Austrian national courts.

¹ [REDACTED] is a private limited company incorporated in Malta and operating in the online gaming sector with registration number [REDACTED] and registered address at [REDACTED]

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

³ [REDACTED] is a private limited company incorporated in Malta and operating in the online gaming sector with registration number [REDACTED] and registered address at [REDACTED]

4. According to the complainant, the transfer of his personal data from the controller to [REDACTED] [REDACTED] is not covered by the controller's privacy policy⁴ (the "**Privacy Policy**"). Furthermore, the complainant argued that he had not given the controller the permission to transfer his personal data.
5. Consequently, the complainant considered this processing activity constitutes an infringement of the provisions of the Regulation, specifically articles 5 and 6 and, or 9 thereof.
6. As supporting documentation, the complainant provided a copy of an objection dated the 10th August 2020 filed by [REDACTED] with the District Court Fünfhaus, Austria, before which the complainant had commenced judicial proceedings against [REDACTED] under the European Small Claims Procedure.
7. On pages 9 and 10 of such documentation, the defendant, [REDACTED], mentioned that the complainant had previously opened a [REDACTED] on the website [REDACTED] operated by the controller, and that he had subsequently requested [REDACTED] a [REDACTED] [REDACTED] based on the alleged illegality of [REDACTED]' operations in Austria, which is the country from where the complainant had placed his bets. In its objection, [REDACTED] also provided that [REDACTED] had agreed to reimburse the amount demanded by the complainant out-of-court, without accepting that his claim was legally grounded.

INVESTIGATION

8. The Commissioner requested the controller to provide its submissions on the allegation raised by the complainant, and in particular: (a) a copy of the policy on the handling of the alleged fraud cases; (b) a copy of the group organisational structure; (c) confirmation of the role of [REDACTED] in relation to the processing activity subject to the complaint; and (d) the legal basis upon which [REDACTED] relied to transfer the complainant's personal data to [REDACTED]. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint, together with the supporting documents attached thereto.

⁴ [REDACTED], last seen on [...].

9. The controller responded to the Commissioner's request by submitting [REDACTED] [REDACTED] group's (the "group") organisational structure as requested. Furthermore, the controller indicated that both companies carry out their [REDACTED] activities under the same group corporate licence.
10. In its submissions, the controller also sustained that the group did not have any policy in place to cater for transfers of personal data other than the compulsory procedures related to fraud, anti-money laundering and [REDACTED] [REDACTED]. According to the controller, in certain instances, such as when a customer initiates litigation against an entity pertaining to the group, intra-group verifications are made to establish whether a [REDACTED] is registered with other entities pertaining to the group to protect its interests.
11. The controller also clarified that [REDACTED] is part of the group and operates under the corporate group licence, but it remains a controller on its own right.
12. The controller held that by registering as a customer of [REDACTED] the complainant infringed clause 5.13 of the terms and conditions which stipulates that the residents of any jurisdiction where their participation would be in conflict with any applicable law or any other rules, including those relating to [REDACTED], are prohibited from accessing or using the [REDACTED] website, app/s and games from such jurisdictions.
13. According to the controller, the fact that the complainant registered an account with [REDACTED] [REDACTED] after having instituted legal proceedings against the controller in Austria alleging the illegality of the controller's [REDACTED] services offer in Austria, constitute an illegal and fraudulent activity on the part of the complainant.
14. In this regard, the controller mentioned that pursuant to recital 47 of the Regulation, the prevention of fraud is an interest which is *per se* considered legitimate. The controller also provided that it has a legitimate interest within the meaning of article 6(1)(f) of the Regulation to use such information to protect the group in judicial proceedings, and that pursuant to the same recital, such legitimate interest is extended to a controller to which the personal data may be disclosed.

15. Thereafter, through the Austrian SA, the Commissioner granted the complainant the right to be heard by presenting the legal arguments of the controller. In this respect, the complainant was provided with all the submissions provided until the date of the request for submissions.
16. The complainant refuted the arguments of the controller on the basis that his behaviour was illegal or fraudulent, given that:
 - a. the controller never took any action against him in that regard;
 - b. the controller did not prevent him from opening a [REDACTED] account with [REDACTED] and from placing [REDACTED] therein;
 - c. the Austrian courts decided to dismiss his claim against [REDACTED] for abuse of rights and accordingly, the complainant stressed that in his opinion, abuse of right is not fraud.
17. The complainant emphasised that the reason why he lost his lawsuit against [REDACTED] was the allegedly unlawful transfer of his personal data from [REDACTED] to [REDACTED].
18. On a final note, the complainant held that the controller's operations in Austria were illegal because they were based on null and void contracts, and that he could not be expected to be aware that [REDACTED] formed part of the complex corporate structure of [REDACTED] given that this information was not mentioned in the Privacy Policy.

LEGAL ANALYSIS AND DECISION

19. As the first step of this legal analysis, the Commissioner sought to establish whether the controller had indeed transferred personal data concerning the complainant to the third party, [REDACTED].

In this regard, the Commissioner carefully examined the corporate group structure submitted by the controller, and it was established that [REDACTED] and [REDACTED] are both subsidiaries of [REDACTED] [REDACTED] and form part of the same group of companies. Additionally, the Commissioner carried out the necessary verifications by consulting the Malta [REDACTED]

Authority's licence register⁵, and confirmed that the two (2) companies operate under the same corporate licence. Notwithstanding this, it is imperative to emphasise that, for the purpose of data protection legislation, the two (2) companies are deemed to be separate controllers.

20. After having examined the information used by [REDACTED] in its objection filed before the Austrian Courts, the Commissioner determined that the controller had in fact transferred certain personal data pertaining to the complainant to [REDACTED]. This was also implicitly acknowledged by the controller in its submissions provided to the Commissioner during the course of the investigation.

Lawfulness of the Processing

21. In this respect, the Commissioner notes that the principle of lawful processing, which is one of the data protection principles, requires that every data processing operation has a lawful ground for processing. In this regard, article 6(1) of the Regulation stipulates what may constitute such a legal basis, taking also into consideration all the other core principles for processing personal data as set out in article 5 of the Regulation.
22. The Commissioner therefore proceeded to examine article 6(1)(f) of the Regulation, which is the legal basis invoked by the controller in relation to the transfer of the complainant's personal data to [REDACTED]
23. Such provision provides that the processing shall be lawful as long as it "*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 [...]*" [emphasis has been added].
24. Within this context, the Commissioner examined the judgments⁶, delivered by the Court of Justice of the European Union (the "**CJEU**"), whereby it elaborated on the concept of the three-part test and stated that "*Article 7(f) of Directive 95/46 lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed;*

[REDACTED] last accessed on 4th May 2022.
⁶ Rigas satiksme, C-13/16, paragraph 28 and TK v Asociația de Proprietari bloc M5A-ScaraA, Case C-708/18, paragraph 40.

second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.” [emphasis has been added].

25. In this respect, the Commissioner assessed the present case in the light of the three (3) cumulative conditions as laid down by the CJEU. All the three (3) conditions identified by the Court need to be present for the processing to be lawful: (i) the existence of a legitimate interest justifying processing; (ii) the necessity of processing for the realisation of the legitimate interest; and (iii) the prevalence of that interest over the rights and interests of the data subject, which calls for balancing of interests.
26. First, the processing is conditional upon the existence of the legitimate interest of the controller or of a third party. The Regulation does not define legitimate interest and thus, it is for the controller to determine whether there is a legitimate aim that could justify an interference with the right to the protection of personal data.
27. The Commissioner interprets “*interest*” to be the broader stake that a controller may have in the processing, or the benefit that the controller or third parties may derive from such processing. This interpretation is substantiated by the recitals of the Regulation, which provide some non-exhaustive examples of situations in which legitimate interest could exist and this could be processing for the purpose of preventing fraud, processing for direct marketing purposes, the transmission of certain data within groups of companies and processing for the purpose of ensuring network and information security. Furthermore, the case-law of the CJEU held that transparency or the protection of the property, health and family life, are legitimate interests⁷.
28. Additionally, the interest has to be “lawful”, which means that the interest pursued cannot go against a legislative measure. In the present case, the legitimate interest at stake is that of a third party, ██████████, specifically to defend itself in judicial proceedings instituted by the complainant. Consequently, the third party which forms part of the same group as the controller, exercised its fundamental right of defence, as enshrined in article 48 of the Charter of Fundamental Rights of the European Union.

⁷ Volker and Markus Schecke and Eifert, Case C-92/09 and C-93/09, paragraph 77 & Rynes, Case C-212/13, paragraph 34.

29. It is hereby significant to underline that the Court of Justice of the European Union in the Rīgas ruling held that “[a]s regards the condition relating to the pursuit of a legitimate interest, as the Advocate General stated in points 65, 79 and 80 of his Opinion, there is no doubt that **the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest**”⁸ [emphasis has been added].
30. The Commissioner highlights that there shall be a substantiated link between the processing activity and the legitimate interest pursued by the third party concerned. In the case at present, the Commissioner considered that the interest pursued by [REDACTED], to which the personal data have been disclosed, is deemed to be sufficiently clear, articulated and specific.
31. In relation to the second condition, the Commissioner examined if the processing goes beyond what is necessary, and therefore assessed if the processing activity was necessary for the purpose of the attainment of the legitimate interests at issue.
32. The CJEU in its judgment Huber⁹ established that the condition of ‘necessity’ has its own independent meaning, which shall reflect the spirit and scope of the data protection legislation. Accordingly, the Commissioner notes that the principle of data minimisation as laid down in article 5(1)(c) of the Regulation requires that the processing shall be adequate, relevant, and limited to what is necessary in relation to the purpose of the processing. It therefore follows that the processing of personal data shall be limited to what is plausibly necessary¹⁰ to pursue a legitimate interest and therefore, there shall be a connection between the processing and the interest pursued. For this purpose, any data that is not directly linked to obtaining, realising or otherwise accomplishing the legitimate interests pursued is not lawfully processed.

⁸ Judgment of the Court (Second Chamber) of 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, C-13/16, ECLI:EU:C:2017:336, para. 26.

⁹ Heinz Huber vs Bundesrepublik Deutschland CJEU C-524/06, 18 December 2008, para. 52.

¹⁰ Judgment of the European Court of Human Rights in case Silver & Others v United Kingdom of 25 March 1983, para 97 discussing the term 'necessary in a democratic society': “*the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"*”

33. After assessing the circumstances of the case, the Commissioner established that the processing activity conducted by the controller was proportionate and adequately targeted to meet the interests of the third party, specifically, the right of defence.
34. Finally, article 6(1)(f) of the Regulation calls for a balancing test, which requires that the controller assesses whether the legitimate interest pursued by the third party is overridden by the interests or fundamental rights and freedoms of the complainant. In this respect, account shall be taken, *inter alia*, of the nature of the legitimate interest being pursued, the nature of the personal data at issue, and the impact on the data subject. In relation to the latter point, the Article 29 Working Party¹¹ clarifies the purpose of article 6(1)(f) of the Regulation is not to prevent any negative impact on the data subject, but to prevent any disproportionate impact. In the case at present, the complainant contended that the Court rejected his claims against [REDACTED] [REDACTED] as a result of the unlawful transfer of his personal data from [REDACTED] to [REDACTED], however, the Commissioner could not consider this as a relevant consideration which tips in favour of the complainant.

Information Obligation

35. Consequently, the Commissioner proceeded to examine the Privacy Policy available on the controller's website in order to establish whether the controller informed the data subject about the possibility of sharing information with other companies forming part of the same group in case of judicial proceedings instituted against one of the companies.
36. Accordingly, article 13(1)(b) of the Regulation states that controller shall, at the time when personal data are obtained, provide "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*". In addition, pursuant to article 13(1)(e) of the Regulation, the controller shall provide information in relation to "***the recipients or categories of recipients of the personal data, if any***" [emphasis has been added].
37. Article 4(9) of the Regulation defines a "*recipient*" as "*a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third*

¹¹ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

party or not." In this regard, the definition of "*recipient*" encompasses other controllers to whom personal data have been disclosed by the controller.

38. After closely examining the Privacy Policy, particularly '*Section 5 – Recipients of Your Personal Data*', the Commissioner noted that the controller does not provide any information in relation to the sharing of personal data among the group of companies for the purpose of establishment, exercise or defence of a legal claim and for legal proceedings which may be instituted under any law, as in fact was confirmed by the controller in its submissions provided to the Commissioner.

On the basis of the foregoing considerations, the Commissioner hereby decides that:

- a. **the transfer of the complainant's personal data by the controller to [REDACTED] was lawful on the basis of article 6(1)(f) of the Regulation; and**
- b. **the controller infringed article 13(1)(c) and (e) of the Regulation, when it failed to provide the complainant with information regarding the possible disclosure of his personal data within the group of companies and the purpose of the processing for which the personal data are intended as well as the legal basis for such processing.**

By virtue of article 58(2)(b) of the Regulation, the controller is hereby being served with a reprimand for having infringed the above-mentioned provisions.

Pursuant to article 58(2)(d) of the Regulation, the controller is hereby being ordered to amend the Privacy Policy, by including the following information:

- a. **the recipients, or categories of recipients of the personal data;**
- b. **the legal basis of the processing; and**
- c. **the purpose of the processing.**

This order shall be implemented within ten (10) days from the date of receipt of this legally-binding decision and the controller is requested to inform the Commissioner with the action taken to comply with such order immediately thereafter.

In terms of article 78 of the Regulation, as further implemented under Part VII of the Data Protection Act (CAP. 586 of the laws of Malta), any party to this decision shall have the right to an effective judicial remedy by filing an appeal in writing before the Information and Data Protection Appeal Tribunal within twenty (20) days from the service of this decision¹².



(Signature

Date: 2022.06.28
10:18:46 +02'00'



Information and Data Protection Commissioner

¹² More information about the Tribunal and the appeals procedure is accessible at <https://idpc.org.mt/appeals-tribunal/>

Information and Data Protection Commissioner

CDP/IMI/LSA/10/2020

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. Reference is made to the complaint lodged by [REDACTED] (the “**complainant**” or the “**data subject**”) on the 4th July 2019 against [REDACTED] (the “**controller**” or “[REDACTED”]), which has been referred to the Information and Data Protection Commissioner (the “**Commissioner**”) by the Norwegian supervisory authority (the “**Datatilsynet**” or the “**Norwegian DPA**”), acting as the concerned supervisory authority.
2. The Norwegian DPA informed the Commissioner about the case on the 17th March 2020, when the Norwegian DPA initiated the procedure pursuant to article 56 of the General Data Protection Regulation² (the “**Regulation**”). Following an assessment carried out by the Commissioner, it was determined that the controller has its main establishment in Malta.
3. The complainant held an account with [REDACTED] and his complaint relates to the fact that the controller requested him to provide a copy of the bank’s transaction history for the months of May and June 2019 as a way to sufficiently demonstrate that he has not received the [REDACTED]. The complainant considered this request to be excessive and unnecessary. Additionally, he complained about the lack of proper information in relation to who is the [REDACTED] provider, leading him to have no control over who has access to his personal data and how it is stored, managed and used.

¹ [REDACTED] is a private limited company registered under the laws of Malta with number [REDACTED] having its registered address at [REDACTED].

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

INVESTIGATION

4. Pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide its submissions in relation to the allegations raised by the complainant. In terms of this Office's internal investigation procedure, the controller was provided with a copy of the complaint together with the supporting documents.
5. On the 2nd April 2020, the controller submitted the following principal legal arguments, together with supporting evidence³, for the Commissioner to consider during the legal analysis of this case:
 - a. that after the complainant was informed via an automated message that the [REDACTED] has been affected pursuant to its standard procedure, the complainant claimed that he did not receive his [REDACTED], a total sum of [REDACTED];
 - b. that the customer support sent the complainant an excel file to prove that the [REDACTED] was processed, including a record of the date of w[REDACTED] and the amount [REDACTED]
 - c. that the complainant did not deem this to be sufficient and therefore, the controller had to find another way to verify if the complainant had received the [REDACTED] and accordingly, requested the customer to provide a bank statement, leaving the details relating to incoming transactions with an amount close to [REDACTED] visible, after the complainant objected to send his bank statements;
 - d. that the controller requested the bank statements that would present the description of transactions for the following two (2) reasons: (i) the controller has a legitimate interest, particularly, to ensure with reasonable certainty that this is not a fraudulent claim; and (ii) the controller had previously encountered situations where customers were not recognising transactions due to a change in the billing descriptor and therefore, the controller wanted to verify whether this was also the issue in this particular case;

³ Controller's confirmation of [REDACTED], Excel file with [REDACTED] history, complainant's bank account screenshots and original transcripts of communication between the controller and the complainant.

- e. that the controller pointed out that the complainant provided only the information limited to dates and amounts [REDACTED], and therefore, at no time were full bank statements provided to the controller; and
 - f. that the controller outlined that it is the standard procedure to only request the minimum necessary information as required on ad hoc basis and in this specific case, due to issue which the controller was experiencing with [REDACTED] providers and potential change in the billing descriptor, the controller had determined that the most effective way to verify [REDACTED] was to request a bank statement from the complainant.
6. The Commissioner verified from the transcript of the communication exchanged between the controller and the complainant that the controller had sent the [REDACTED] reference number to the complainant. However the complainant was not able to find any [REDACTED] bearing this reference number when searching through the transactions of his bank account.
7. It also appears that on the 26th June 2019, the complainant copied and pasted a list containing some transactions as shown in his bank account and sent it to the controller by means of an email. The controller replied on the 27th June 2019 and provided the complainant with clearer instructions of what information was required to investigate the matter further: “*Please attach screenshots showing the full website, such as URL and the bank logo, including your bank account number and your full name. We would like the 2 last transactions on the first document that you submit to appear in the second document, so that the transactions overlap. Please note that we do not accept images of your transaction history from a cell phone. We prefer that you attach a PDF document reflecting your bank account*”.
8. Following a request made by the Commissioner, by means of an email dated the 23rd July 2021, the controller explained that “*this specific [REDACTED] request did not trigger any identity verification procedures since, after assessing the customer request, operational teams did not identify flags that would require further verifications... the issue at hand was not the customer identity but whether the transaction was indeed conducted or not...the main issue, in this case, was whether the customer indeed received the [REDACTED] on her bank account. The customer had requested a [REDACTED], which was processed...However, despite all proofs of [REDACTED] provided by the customer support team, the customer claimed that the [REDACTED] had not been received. Such queries can happen as customers sometimes fail to identify [REDACTED], due to different descriptors used by*

payment service providers. However, ...since after all regular confirmations that were sent (OMS, transaction history, etc.), in this case, the customer was still not satisfied as she still claimed that the [REDACTED] was not visible on her bank statements. Therefore, the only last resort to prove what factually happened was to request her bank statements to verify whether the transaction was received or not on her bank account". The controller added that ' [REDACTED] believes that the request for such information is proportional in view that it is within legitimate interest to ensure that this is not a fraudulent claim, and also since from experience we are aware that certain payment providers can change billing descriptions."

9. On the 27th July 2021, the controller confirmed that, even though it was not possible to make sure whether the [REDACTED] was received by the complainant given that the requested bank statement was never provided, the controller wanted to trust the complainant's good faith and decided to proceed with a new withdrawal⁴ "...but now via a different payment method. According to [the controller's] records, he got that payment".
10. After the new [REDACTED] was processed, the controller never heard back from the complainant and presumed that the [REDACTED] was safely received and thus, the complainant was satisfied.
11. On the 29th October 2021, the Commissioner requested the controller to provide evidence of the issues encountered with some payment providers at the time when the complainant requested his [REDACTED]. In its reply received on the 3rd November 2021, the controller provided evidence, in the form of a screen shot, "showing execution of the transaction" by the service provider. Moreover, the controller further explained that "*the payment provider successfully received the instruction for [REDACTED], therefore, we did not see any issue that this customer might have had with the payment provider. However, since the customer was claiming that he did not get this payment, we thought that he might be having the same problem with identifying the billing descriptors, which other customers were reporting to us (customers were not seeing a proper description on their bank statement which clearly shows from where the funds were coming, as some payment service providers were using different descriptors)*".
12. The controller further added that "[s]ince from our end we did, and to this date, do not have any proof that there was a problem with this transaction, but rather customer is the one

⁴ The controller " [REDACTED] the funds to the customer account on 03.04.2020 and the customer [REDACTED] the funds on 25.06.2020".

claiming that he did not get the money from us in spite of all evidence provided from our end, our only last resort to prove what factually happened was to request his bank statement. This was necessary to verify whether the transaction was received or not on his bank account (by checking whether any date and amount matched the [REDACTED] paid from our end, although the description might be different) ”.

LEGAL ANALYSIS AND DECISION

13. For the purpose of this legal analysis, the Commissioner sought in essence, to establish the legal basis upon which the controller relied to request the complainant to provide a copy of his bank transaction history to verify if the [REDACTED] has indeed been received by the complainant and to determine whether the controller has fully complied with its information obligations pursuant to the requirements of the Regulation.

Lawful basis

14. In terms of article 8 of the Charter of Fundamental Rights of the European Union, personal data shall be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. In this respect, the Commissioner notes that the principle of lawful processing, which is one of the data protection principles, requires that every data processing operation has a lawful ground for processing. In this regard, article 6(1) of the Regulation stipulates what may constitute such a legal basis, taking also into consideration all the other core principles for processing personal data as set out in article 5 of the Regulation. Therefore, a controller shall be in a position to identify the appropriate legal basis before the processing activity, which corresponds to the objective and essence of the processing activity.
15. In his analysis, the Commissioner considered the submissions provided by the controller, wherein it argued that it is “*in our legitimate interest to ensure with reasonable certainty that this is not a fraudulent claim*” and therefore the request to provide a copy of the bank statement was based on article 6(1)(f) of the Regulation.
16. In this regard, the Commissioner assessed article 6(1)(f) of the Regulation, which states that the processing shall be lawful if it “*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...”.

17. Within this context, the Commissioner examined the judgments⁵, delivered by the Court of Justice of the European Union (the “Court”), whereby it elaborated on the concept of the three-part test and stated that “*Article 7(f) of Directive 95/46 lays down **three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence.***” [emphasis has been added].
18. Accordingly, the Commissioner assessed the present case in light of the three (3) cumulative conditions as laid down by the Court. All the three (3) conditions identified by the Court need to be present: (i) the existence of a legitimate interest justifying processing; (ii) the necessity of processing for the realisation of the legitimate interest; and (iii) the prevalence of that interest over the rights and interests of the data subject, which calls for balancing of interests.
19. First, the processing is conditional upon the existence of a legitimate interest of the controller or of a third party. The Regulation does not define legitimate interest and thus, it is for the controller to determine whether there is a legitimate aim that could justify an interference with the right to the protection of personal data.
20. The Commissioner interprets “*interest*” to be the broader stake that a controller may have in the processing, or the benefit that the controller or third parties may derive from such processing. This interpretation is substantiated by the recitals of the Regulation, which provide some non-exhaustive examples of situations in which legitimate interest could exist and this could be processing for the purpose of preventing fraud, processing for direct marketing purposes, the transmission of certain data within groups of companies and processing for the purpose of ensuring network and information security. Furthermore, the case-law of the Court of Justice of the European Union held that transparency or the protection of the property, health and family life are legitimate interests⁶.

⁵ Rigas satiksme, C-13/16, paragraph 28 and TK v Asociația de Proprietari bloc M5A-ScaraA, Case C-708/18, paragraph 40.

⁶ Volker and Markus Schecke and Eifert, Case C-92/09 and C-93/09, paragraph 77 & Rynes, Case C-212/13, paragraph 34.

21. Pursuant to the Guidelines issued by the Article 29 Working Party⁷, the interest is deemed to be ‘legitimate’ if it fulfills the following conditions: (i) it is lawful; (ii) it is sufficiently clearly and articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject; and (iii) represent a real and present interest.
22. The Article 29 Working Party recognises that “*prevention of fraud*” is one of the most common contexts in which the issue of legitimate interest may arise. Additionally, recital 47 of the Regulation provides that the “*processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned*”. It therefore follows that the legitimate interest pursued by the controller is clearly articulated, effective and real, and consequently, justified.
23. In relation to the second condition, the Commissioner examined if the processing goes beyond what is necessary, and therefore assesses if the request made by the controller for a copy of the bank statements that would present a description of transactions, covering the period between the 23rd May 2019 until the 2nd July 2019, was necessary for the purpose of the attainment of the legitimate interest at issue.
24. The Commissioner notes that the principle of data minimisation as laid down in article 5(1)(c) of the Regulation requires that the processing shall be adequate, relevant and limited to what is necessary in relation to the purpose of the processing. It therefore follows that the processing of personal data shall be limited to what is plausibly necessary⁸ to pursue a legitimate interest and therefore, there shall be a connection between the processing and the interest pursued. For this purpose, any data that is not directly linked to obtaining, realising or otherwise accomplishing the legitimate interests pursued is not lawfully processed.
25. Additionally, recital 39 of the Regulation sheds further light on the principle of data minimisation, by stipulating that “[p]ersonal data should be processed only if the purpose of the processing **could not reasonably be fulfilled by other means**”.

⁷ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, adopted on the 9th April 2014.

⁸ Judgment of the European Court of Human Rights in the case Silver & Others v United Kingdom of 25 March 1983, para 97 discussing the term 'necessary in a democratic society': “*the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"....*”

26. The Court of Justice of the European Union in its judgment ‘TK vs Asociația de Proprietari bloc M5A-ScaraA’⁹ states that the second condition relating to the principle of data minimisation “*requires the referring court to ascertain that the legitimate data processing interests pursued by the video surveillance at issue in the main proceedings — which consist, in essence, in ensuring the security of property and individuals and preventing crime — cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.*” [emphasis has been added].
27. In this regard, the proportionality of the data processing should be assessed by taking into account the methods that could be used to effectively achieve the same results whilst limiting the effect on the rights and freedoms of the complainant. On that account, the Commissioner considers that the controller’s approach to shift the burden of proof on the complainant and request him to provide a bank statement showing transactions over a period of time for the purpose of establishing whether a pay-out which they have made, and which they should be able to effectively demonstrate that it has been made, runs contrary to the principle of accountability. This consideration is being made while also taking into account the measures which the controller indeed has at its disposal to check or otherwise verify, internally, but also with other third party service providers with whom they have a contractual agreement involving processing activities of personal data, in this specific case, whether a pay-out to the data subject has been successfully affected or not.
28. After assessing the circumstances of the present case, the Commissioner noted that the request for all the transactions covering the period of over a month is deemed to be excessive as this inevitably leads to the further processing of personal data which are not relevant for attaining the objective of the controller.
29. Finally, article 6(1)(f) of the Regulation calls for a balancing test, which requires that the controller assesses whether the legitimate interest pursued by the third party is overridden by the interests or fundamental rights and freedoms of the complainant. In this respect, account shall be taken, *inter alia*, of the nature of the legitimate interest being pursued, the nature of the personal data at issue, and the impact on the data subject. In relation to the latter point, the

⁹ Case C-708/18, 11th December 2019.

Article 29 Working Party¹⁰ clarifies the purpose of article 6(1)(f) of the Regulation is not to prevent any negative impact on the data subject, but to prevent any disproportionate impact.

30. Pursuant to recital 47 of the Regulation, the existence of a legitimate interest needs a careful assessment, including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The Article 29 Working Party highlights that “*it is important to consider whether the status of the data controller, the nature of the relationship or the service provided, or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use*”.¹¹
31. The recently adopted Guidelines¹² issued by the European Data Protection Board provide that the decisive criterion that should be taken into account by the controller is the intensity of the intervention that the processing poses for the rights and freedoms of the data subject. Within this context, the Commissioner examined the nature of the personal data requested by the controller, which would have led to the disclosure of all the complainant’s banking transactions covering a period that exceeds more than one (1) month, in order to verify whether the complainant has indeed received a [REDACTED] of [REDACTED]. From this data, certain inferences could be made in relation to the financial situation of the complainant, including information in relation to his income and spending habits or patterns. Therefore, after taking into account all the relevant factors which are balanced against the legitimate interest pursued by the controller, the Commissioner considers the significance of the complainant’s fundamental right and determines that the balancing exercise tips in favour of the complainant.

Information Obligation

32. The complainant contended that the controller could potentially share the requested bank transactions with the supplier which the controller refused to identify, and therefore, the complainant alleged he has no control over who has access to his personal data, how his data are managed and stored, or utilised thereafter.

¹⁰ Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.

¹¹ Ibid. 9, page 40.

¹² Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, adopted on the 29th January 2020, para. 32.

33. Accordingly, the Commissioner proceeded to examine the privacy policy on the controller's website¹³ available at the time of the complaint received by this Office to establish that the controller provided information to the data subjects in relation to the recipients to whom the controller might transfer or disclose the personal data at customer registration stage¹⁴. In fact, the Privacy Policy reads as follows: “*Your personal information may be transferred or disclosed (for the purposes described in this policy) to any company within the [REDACTED] and, subject to an appropriate agreement with third parties to process that personal information on our behalf, such as: Our [REDACTED] providers, based on your preferences, to process your [REDACTED] [REDACTED] and [REDACTED]*”.
34. Within this context, the Commissioner considered article 13(1)(e) of the Regulation, which provides that “*where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (e) the recipients or categories of recipients of the personal data, if any*” [emphasis has been added].
35. Thus, the Commissioner examined article 4(9) of the Regulation, which defines a “*recipient*” as “*a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.*” In this regard, the definition of “*recipient*” encompasses processors to whom personal data may be disclosed to, by the controller. The Article 29 Working Party Guidelines on Transparency under Regulation 2016/679¹⁵ provide practical guidance and interpretative assistance on the requirements of article 13, which state the following: “*The actual (named) recipients of the personal data, or the categories of recipients, must be provided. In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients.*”

¹³ [REDACTED]

¹⁴ The customer registration form on [REDACTED] includes a link to the Privacy Policy.

¹⁵ Adopted on 29 November 2017 as last revised and adopted on 11 April 2018.

On the basis of the foregoing considerations, the Commissioner hereby decides that:

- i. by means of the privacy policy made available at registration stage, the controller has informed the complainant about the categories of recipients pursuant to the requirement set forth in article 13(1)(e) of the Regulation; and
- ii. the request of the controller is deemed to be excessive and unnecessary for the purpose of attaining its legitimate interest, and therefore, not lawful pursuant to article 6(1) of the Regulation. Consequently, in terms of article 58(2)(b) of the Regulation, the Commissioner is hereby issuing a reprimand to the controller and warned that in the event of a similar infringement, he will take the appropriate corrective action in terms of his powers at law.

In terms of article 78 of the Regulation, as further implemented under Part VII of the Data Protection Act (CAP. 586 of the laws of Malta), any party to this decision shall have the right to an effective judicial remedy by filing an appeal in writing before the Information and Data Protection Appeal Tribunal within 20 days from the service of this decision¹⁶.



Digitally signed by



(Signature)

Date: 2022.09.06
11:30:14 +02'00'

¹⁶ More information about the Tribunal and the appeals procedure is accessible at <https://idpc.org.mt/appeals-tribunal/>

Information and Data Protection Commissioner

CDP/IMI/LSA/22/2021

[REDACTED]

vs

[REDACTED]

COMPLAINT

1. On the 24th June 2021, [REDACTED] (the “complainant”) lodged a complaint with Österreichische Datenschutzbehörde, the Austrian Supervisory Authority, against [REDACTED] [REDACTED]¹ (the “controller”) pursuant to article 77(1) of the General Data Protection Regulation² (the “Regulation”).
2. The complainant contended that, on the 5th May 2021, she had exercised the right to access her personal data in accordance with article 15 of the Regulation. However, the controller failed to provide the complainant with information about the action taken within the time-frame stipulated by law. The complainant further argued that she was not informed if the controller needed an extension to reply to her request.
3. On the 22nd September 2021, the Austrian Supervisory Authority informed the Information and Data Protection Commissioner (the “Commissioner”) about the complaint pursuant to article 56(3) of the Regulation. Following an assessment carried out by the Commissioner, it was established that the controller has its main establishment in Malta. Thus, the Commissioner proceeded to handle the case as the lead supervisory authority.

¹ [REDACTED] is a private limited company registered under the laws of Malta with number [REDACTED], having its registered address at [REDACTED].

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

INVESTIGATION

4. Pursuant to article 58(1)(a) of the Regulation, the Commissioner requested the controller to provide any information which it deemed necessary and relevant to defend itself against the allegation raised by the complainant. In terms of this Office’s internal investigation procedure, the controller was provided with a copy of the complaint, together with all the supporting documentation, provided by the complainant.
5. On the 2nd December 2021, the controller submitted the following principal legal arguments for the Commissioner, to consider during the legal analysis of this case:
 - a. that, on the 5th May 2021, the controller “*received an email from the lawfirm [REDACTED]
[REDACTED]*”, where “[t]he lawfirm requested access to personal data for the player [REDACTED]”;
 - b. that the controller failed to comply with the subject access request submitted by the complainant within the stipulated time-frame “*due to the massive inundation of data subject access requests that the relevant company has received as of late, thereby not allowing for the company to be able to reply within the stipulated period in this particular case*”;
 - c. that, by means of an email dated the 19th June 2021³, the controller informed the lawyer acting on behalf of the complainant, that her request has been processed and requested confirmation to send the requested data via WeTransfer;
 - d. that the controller did not receive a reply to the email dated the 19th June 2021, and, as a result, the controller did not provide a copy of the personal data undergoing processing to the complainant.

³ The controller provided a copy of the email dated the 19th June 2021 in German (original text) and English (translation). The English translation read “*May we send you the requested data via the service provider "WeTransfer"?*”

LEGAL ANALYSIS AND DECISION

The Timing of the Reply

6. The protection of natural persons in relation to the processing of their personal data is a fundamental right recognised by article 8(1) of the Charter of Fundamental Rights of the European Union. Within this context, the rights of the data subjects as set forth in articles 12 to 22 of the Regulation are the fulcrum of the law, and their role is absolutely crucial to ensure the utmost protection of personal data processed by controllers. In this regard, the Commissioner emphasises the importance attributed to the right of access as laid down in article 15 of the Regulation, in particular, its special feature, which is derived from the fact that it is often a means, prerequisite or condition to enable data subjects to oversee and control their personal data, and consequently, exercise other data subjects, such as the right to erasure or rectification⁴.
7. The right of access as enshrined in article 15 of the Regulation contains three (3) components: (i) confirmation of the processing of personal data; (ii) information about the processing itself; and (iii) access to a copy of personal data undergoing processing. Article 15(1) of the Regulation enables the data subject 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*”, as well as other supplementary information pursuant to article 15(1)(a) to (h) and article 15(2) of the Regulation. Further to this, article 15(3) of the Regulation, which is more prescriptive, states that “*the controller shall provide a copy of the personal data undergoing processing*”.
8. In this connection, article 12 of the Regulation ensures that substantive rights of data subjects are safeguarded by establishing clear, proportionate and effective conditions as to how and when data subjects shall exercise their rights. For this reason, article 12 of the Regulation provides the modalities for the exercise of the data subjects’ rights and establishes an obligation upon the controller to facilitate the exercise of these rights.
9. In particular, article 12(3) of the Regulation aims at ensuring the efficient exercise of information and access rights, and obliges the controller to “*provide information on action*

⁴ CJEU, C-434/16, Nowak, para. 56

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". Within this set timeframe, the controller shall either (i) comply with the request; (ii) extend the deadline to two (2) further months and provide the reasons for such extension; or (iii) refuse to act on the request in terms of article 12(5)(b) of the Regulation and inform the data subject accordingly.

10. On this aspect, with particular reference to the handling of data protection requests, the European Data Protection Board⁵ emphasises that '*[t]he controller shall react and, as a general rule, provide the information under Art. 15 without undue delay, which in other words means that the information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so*".
11. After assessing the circumstances of the case, the Commissioner determined that, on the **5th May 2021**, the complainant exercised her right to access her personal data pursuant to article 15 of the Regulation. In the submissions provided to this Office on the **2nd December 2021**, the controller declared that it had contacted the lawyer of the complainant on the **19th June 2021** and that "*due to the massive inundation of data subject access requests that the relevant company has received as of late, thereby not allowing for the company to be able to reply within the stipulated period in this particular case*". Thus, the Commissioner established that the controller failed to provide information to the complainant on the action taken on the request to access her personal data within one (1) month of receipt of the request.

Making the information available

12. In the email dated the 19th June 2021, the controller informed the complainant that her request has been processed and requested the complainant to confirm whether the response could be sent by means of the service provided by WeTransfer.
13. For this purpose, the Commissioner analysed article 12(1) of the Regulation, which establishes that the information shall be provided, where appropriate, by electronic means, in conjunction with the principle of integrity and confidentiality as set forth in article 5(1)(f) of the Regulation.

⁵ EDPB Guidelines 01/2022 on data subject rights - Right of access - Version 1.0 - Adopted on 18 January 2022 – Paragraph 156

14. In this regard, the Commissioner noted that when the controller makes personal data available to the data subject, this is deemed to be a processing operation, and therefore, the controller is obliged to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing in terms of article 32(1) of the Regulation.

In addition, the Commissioner considered article 15(3) of the Regulation, which states that 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.

15. The Regulation does not specify what is a commonly used electronic form, and thus, there are several conceivable formats that could be used by the controller. However, it is important to ensure that the format must enable the information to be presented in a way that is both intelligible and easily accessible. This naturally means that when the controller chooses the means of how to transmit the electronic file to the data subject, the controller shall ensure that the data subject is able to download the information in a commonly used electronic form.

16. Furthermore, recital 63 of the Regulation establishes that “[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data”.

17. It therefore follows that it is the responsibility of the controller to decide about the appropriate form in which the personal data shall be provided to the data subject and this is also in light of the accountability principle as held in article 5(2) of the Regulation.

On the basis of the foregoing considerations, the Commissioner hereby decides that the controller infringed:

- i. **article 12(3) of the Regulation, when it failed to provide the complainant with information on the action taken on her subject access request within one (1) month from the date of receipt of request; and**

- ii. **article 15(1), article 15(2) and article 15(3) of the Regulation, when it failed to provide the complainant with a copy of her personal data undergoing processing and the information concerning the processing.**

By virtue of article 58(2)(b) of the Regulation, the controller is hereby being served with a reprimand. Furthermore, in terms of article 58(2)(c) of the Regulation, the controller is hereby being ordered to comply with the request and provide the complainant with the information prescribed under article 15(1)(a) to (h) and article 15(2) of the Regulation and also with a copy of her personal data undergoing processing at the time of submitting the request pursuant to article 15(3) thereof.

The controller shall comply with this order within ten (10) days from the date of receipt of this legally binding decision. Non-compliance with the order of the Commissioner within the stipulated timeframe shall result in the imposition of an administrative fine in terms of article 83(6) of the Regulation.

In terms of article 26(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), any party to this decision shall have the right to an effective judicial remedy by filing an appeal in writing before the Information and Data Protection Appeal Tribunal within twenty (20) days from the service of this decision⁶.

[Redacted]
[Redacted]
(Signature)

Digitally signed
[Redacted]
(Signature) Date:
2022.12.27
12:45:50 +01'00'

[Redacted]
Information and Data Protection Commissioner

⁶ More information about the Tribunal and the appeals procedure is accessible on <https://idpc.org.mt/appeals-tribunal/>



[REDACTED]

Date
10 December 2020

Our reference

Contact person

Subject

Decision to impose an administrative fine

Dear [REDACTED],

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) (hereinafter: the AP) has decided to impose an **administrative fine of € 475,000** on [REDACTED] (hereinafter: [REDACTED]). The AP considers that [REDACTED] infringed Article 33(1) of the General Data Protection Regulation (*Algemene Verordening Gegevensbescherming*) (hereinafter: GDPR) from 16 January 2019 to 6 February 2019, because [REDACTED] failed to notify the AP of a personal data breach within 72 hours of becoming aware of it.

This decision is explained in more detail below. Section 1 contains an introduction and Section 2 describes the legal framework. In Section 3, the AP assesses its authority, the processing responsibility and the infringement. Section 4 elaborates on the level of the administrative fine and Section 5 contains the operative part and the remedy clause.



Date
10 December 2020

Our reference
[REDACTED]

1. Introduction

1.1 Legal entities concerned

[REDACTED] is a private limited liability company with its registered office at [REDACTED]. [REDACTED] was incorporated on [REDACTED] and entered in the register of the Chamber of Commerce under number [REDACTED]. [REDACTED] provides an online platform through which [REDACTED], such as accommodations, can offer their products and services and users of the platform can then reserve these products and services.

[REDACTED] is, through various Dutch and English legal entities, an indirect 100% subsidiary of [REDACTED], which is listed on the American NASDAQ Stock Market. In 2019, [REDACTED] had a sales volume of USD 15.1 billion (EUR 13,727,410,000) and a net result of USD 4.9 billion (EUR 4,454,590,000) according to its public and consolidated financial statements.

1.2 Reason for this investigation

On 7 February 2019, [REDACTED] reported a personal data breach to the AP. An unknown third party had gained access to a reservation system of [REDACTED] by pretending to be an employee of [REDACTED] to various accommodations. As a result, the personal data of various data subjects who had made hotel reservations via the [REDACTED] platform were compromised. Because [REDACTED] indicated on the notification form that it had discovered the personal data breach on 10 January 2019, the AP commenced an investigation into [REDACTED]'s compliance with Article 33(1) of the GDPR.

1.3 Course of the investigation

By letter dated 12 February 2019, the AP sent a request for information to [REDACTED]. This request was also sent by e-mail dated 26 February 2019.

On 27 February 2019, [REDACTED] provided substantive information in connection with the aforementioned personal data breach notification.

By letter dated 1 March 2019, [REDACTED] responded in writing to the request for information of 12 February 2019.

By letter dated 6 March 2019, the AP sent an additional request for information to [REDACTED].

By letter dated 13 March 2019, [REDACTED] responded in writing to the request for information of 6 March 2019.

By e-mail dated 19 March 2019, the AP sent an additional request for information to [REDACTED].



Date
10 December 2020

Our reference
[REDACTED]

By e-mail dated 19 March 2019, [REDACTED] sent the requested information and an additional document to the AP.

Due to the cross-border nature of the case, the AP informed the other supervisory authorities of the case on 19 March 2019, informing them that the AP would act as lead authority since the head office of [REDACTED] is located in the Netherlands.

By letter dated 16 July 2019, the AP informed [REDACTED] of its enforcement intention and provided it with the investigation report, thereby giving [REDACTED] the opportunity to express its views. By letter dated 3 September 2019, [REDACTED] expressed its views in writing with regard to this intention and the report on which it is based.

On 23 October 2020, the AP submitted a draft decision to the relevant supervisory authorities in conformity with Article 60 of the GDPR. No objections to this decision have been received.

2.Legal framework

2.1 Scope of the GDPR

Pursuant to Article 2(1) of the GDPR, this decision applies to the processing of personal data wholly or partly by automatic means and to the processing of personal data which form part of a filing system or are intended to form part of a filing system.

Pursuant to Article 3(1) of the GDPR, this decision applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

In this decision, pursuant to Article 4 of the GDPR, the following terms have the following meanings:

1. "Personal data": any information relating to an identified or identifiable natural person (data subject); [...].
2. "Processing": any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automatic means [...].
7. "Controller": the [...] legal person [...] which, alone or jointly with others, determines the purposes and means of the processing of personal data; [...].
12. "Personal data breach": 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;
23. "Cross-border processing": [...] b) processing of personal data which takes place in the context of the activities of a single establishment of a controller [...], but which substantially affects or is likely to substantially affect data subjects in more than one Member State.



Date

10 December 2020

Our reference

[REDACTED]

2.2 Notification of a personal data breach

Pursuant to Article 4(12) of the GDPR, a “personal data breach” means: 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.

Pursuant to Article 33(1) of the GDPR, a 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 (...). If the notification to the supervisory authority is not made within 72 hours, it must be accompanied by the reasons for the delay.

2.3 Competence of the lead supervisory authority

Pursuant to Article 55(1) of the GDPR, each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Pursuant to Article 56(1) of the GDPR, and without prejudice to Article 55, the supervisory authority of the main establishment or of the sole establishment of the controller (...) shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller (...) in accordance with the procedure provided in Article 60.

3. Assessment

3.1 Competence of the AP

In this case, the processing of personal data by [REDACTED] had a significant impact on data subjects in more than one Member State.¹ This constitutes cross-border processing within the meaning of Article 4(23)(b) of the GDPR. Since [REDACTED]'s main establishment is in [REDACTED], the AP determines that it is competent to act as the lead supervisory authority in accordance with Article 56 of the GDPR.

3.2 Processing of personal data

According to Article 4(1) of the GDPR, personal data means any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to one or more factors specific to the physical or physiological identity of that natural person.

¹ See paragraph 3.4.2.



Date
10 December 2020

Our reference
[REDACTED]

Article 4(2) of the GDPR defines the concept of processing as any operation or set of operations performed on personal data, such as the collection, recording, storage, retrieval, consultation or use of such data.

[REDACTED] offers an online booking platform through which [REDACTED], such as accommodation providers and other providers, can offer accommodation, flights, rental cars and day trips to users. Through the platform, users can search for and make reservations for accommodation and day trips. When making a reservation through the [REDACTED] platform, a data subject enters personal details such as his/her contact, reservation and payment details. [REDACTED] then provides the details of this reservation to the [REDACTED] via [REDACTED] Extranet.² [REDACTED]'s Extranet is an online administrative dashboard with secure access. In addition to access to reservation details in the Extranet, [REDACTED] have access to all information displayed on the [REDACTED] page at [REDACTED], including payment options and policies. To gain access to the Extranet, a [REDACTED] must enter a username, password and a two-factor authentication pin code. When it has logged on to the [REDACTED], a [REDACTED] can consult the necessary reservation details of the guests.

[REDACTED] called in its Security Team in response to the breach, which found that an unknown third party had gained access to [REDACTED]'s Extranet. The findings of the Security Team have been recorded in a Security Incident Summary report. The Security Incident Summary report dated 28 February 2019, which is included in the file, shows that the following details of guests that were stored in the Extranet were compromised: first name, surname, address, telephone number, check-in and check-out date, total price, reservation number, price per night, any correspondence between the accommodation and the guest and, with regard to 283 data subjects, their credit card details including the card verification code of 97 of these data subjects.³

The reported breach of personal data by [REDACTED] therefore includes names, addresses, telephone numbers and credit card details of hotel guests. As this concerns information on identified or identifiable natural persons, the aforementioned data can be considered as personal data as defined in Article 4(1) of the GDPR.

The AP has determined that personal data is processed through the Extranet: these data are recorded, stored and further accessed through the Extranet. All the processing on the Extranet constitutes the processing of personal data as defined in Article 4(2) of the GDPR.

3.3 Controller

In the context of the question of who can be held responsible for an infringement of the GDPR, it is necessary to determine who can be considered as the controller as defined in Article 4(7) of the GDPR. It is important to ascertain who determines the purpose and means of processing personal data, which in this case is the processing of personal data of data subjects using the [REDACTED] platform.

² File document 1: notification of a personal data breach 7-2-2019, p3.

³ File document 9, [REDACTED]'s replies to requests for information, Appendix 5.



Date

10 December 2020

Our reference

[REDACTED]

The AP is of the opinion that [REDACTED] determines the purpose and means of processing personal data relating to reservations made via [REDACTED].com and then processed via [REDACTED]'s Extranet. The AP explains this as follows.

[REDACTED]'s Privacy Statement, as posted on its website, details the personal data processed by [REDACTED] and the reasons why and the manner in which these data are processed. The Privacy Statement mentions that [REDACTED] shares data with third parties, including the [REDACTED]. The fact that the data is shared with the [REDACTED] via the Extranet is demonstrated by [REDACTED]'s notification of the breach on 7 February 2019 and the views expressed by [REDACTED].⁴ The Privacy Statement also explicitly states that the processing of the aforementioned personal data is performed by [REDACTED] ([REDACTED], the Netherlands).⁵

In addition, [REDACTED] implements security for the Extranet by taking security measures for access control such as the two factor authentication, the code for which is also generated by [REDACTED].⁶ In addition to other security measures, [REDACTED] has set up a data breach notification procedure for incidents involving the Extranet.⁷

On the basis of the above, the AP therefore ascertains that [REDACTED] determines the purpose and means of the processing of personal data relating to reservations made through [REDACTED]'s platform and processed via the Extranet (a system used and managed by [REDACTED]).

On the one hand, [REDACTED] has argued that it is the controller with regard to customer data processed in connection with its platform.⁸ On the other hand, [REDACTED] states that [REDACTED] act as the controller for the customer data made available through the Extranet and that [REDACTED] does not consider itself responsible for data processing activities of [REDACTED].⁹

The fact that [REDACTED] can also (physically) process personal data on the Extranet, does not alter the fact that [REDACTED] is responsible for the processing of personal data on the Extranet. This means that it is also responsible for what happens to the personal data on the Extranet. [REDACTED]'s argument is therefore unfounded.

The fact that [REDACTED] also sees itself as the processor of personal data processed through the Extranet is also demonstrated by the fact that [REDACTED] notified the AP of the personal data breach on 7 February 2019 and that [REDACTED] expresses in its views that it is the controller in respect of customer data processed through its platform.¹⁰

⁴ File document 20: investigation report, marginal 17 ff., views expressed in marginal 2.3 ff.

⁵ Under the heading 'Who is responsible for the processing personal data on the [REDACTED] and how to reach us'.

⁶ Views expressed, marginal 2.5.

⁷ Views expressed, marginals 2.6, 3.2 and 3.3.

⁸ Views expressed, marginal 2.2.

⁹ Views expressed, marginal 2.3.

¹⁰ Views expressed, marginal 2.2.



Date

10 December 2020

Our reference

[REDACTED]

On the basis of the above, the AP ascertains that [REDACTED] is the controller within the meaning of Article 4(7) of the GDPR.

3.4 Infringement of breach notification obligation

3.4.1 Introduction

Article 33(1) of the GDPR provides 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 (...), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, it must be accompanied by the reasons for the delay.

In this section, the AP will first outline the facts and then assess whether [REDACTED] should have reported the personal data breach to the supervisory authority in a timely manner.

3.4.2 The facts

9 January 2019

On 9 January 2019, an [REDACTED]¹¹(I) in the United Arab Emirates informed a [REDACTED] by e-mail that a guest had complained that they had been contacted by an unknown party posing as an employee of the accommodation with a report that their credit card was not working and whether the guest wanted to provide his date of birth or other bank card details so that a reserved overnight stay could be paid for. In his e-mail message to [REDACTED], the accommodation manager asked [REDACTED] to investigate the incident since the accommodation does not have access to customers' e-mail addresses via the Extranet and he thinks that there is probably a data breach at [REDACTED] because the unknown party was aware of the reservation made at the accommodation through [REDACTED]'s platform.

E-mail of 9 January 2019 18:00 hours

"Good Afternoon [...],

We received a complaint from a guest stating that he had provided his personal information and credit card information to a 'stranger' posing as a Reservations employee of our property [...]. In the 1st attachment a person by the name of [REDACTED] had directly email the guest (from a Hotmail account) requesting his credit card and personal info to pay for his booking. We are not sure if the guest had sent the details over. We got to know when someone from [REDACTED] called the property to check if anyone had sent the email. We contacted the guest via the phone number listed in the reservation form – he forwarded the [REDACTED]'email to us. As we do not get guest email address from the extranet, the issue here is likely to be from [REDACTED]. We don't know how this [REDACTED] managed to get hold of the guest email and that he had made a booking at our property from [REDACTED]. Can you review and share the outcome with us. Guest has the perception and understanding that we had leaked the information which is not true. Our brand confidence is at stake here, so is [REDACTED].

Kind Regards [...]"

¹¹ In other words: a [REDACTED].



Date

10 December 2020

Our reference

[REDACTED]

The e-mail that the data subject received from the unknown third party was attached to this e-mail. It appears from this e-mail that the unknown third party was trying to obtain personal and/or payment details using the reservation details of the data subject.

E-mail of 8 January 2019 22:32 hours

"Dear sir

My name is [...] and this email is regarding your booking in our hotel. We got your email address from your office actually sir your bank card is not working. Every time we attempted the payment it on terminal it is asking for card holder date of birth. Kindly provide us with your date of birth or a different card no so we can take the initial deposit of 1 night in order to guarantee the booking the rate for 1st night is 450 emarati dirhams.

Many thanks

[...]

Reservations department"

13 January 2019

On 13 January 2019, the same accommodation (I) informed the abovementioned [REDACTED]

[REDACTED] that the same type of complaint has been received from another guest. An unknown party had made itself known to the guest - this time by telephone - on behalf of [REDACTED], trying to obtain his credit card and personal details.

E-mail of 13 January 2019 10:18 hours

"Subject: RE: [External Fraud] / Leaked Guest Information / URGENT

Hi [...]

We receive a complaint from another guest...this time someone claiming to be from [REDACTED] (UK number) called the guest and was trying to get his cc and personal details for 1 night charge.

I am not sure if the guest provided his details, but he contacted us which we clarified the same (similar clarification as our 1st case). We had requested the guest to call [REDACTED] instead.

We had taken precautions by changing all our logins (for those who has access) last week Thursday.

Booking no. [...]

Regards

20 January 2019

On 20 January 2019, accommodation I reported that a third guest had complained that he had been contacted by telephone asking for his credit card details to be passed on. The accommodation manager informed [REDACTED]'s [REDACTED] that, given the seriousness of the situation, the issue will be forwarded to the head office.

E-mail of 20 January 2019 17:14 hours

"Subject: RE: [External Fraud] / Leaked Guest Information / URGENT



Date
10 December 2020

Our reference
[REDACTED]

[...]

Hi [...]

We receive another complaint from a guest about someone calling them to get cc details. Below is his booking – we have advised him to contact [REDACTED].

As it looks serious now, we are escalating the issue to our head office in Singapore.

Kind regards,

[...]

Also on 20 January 2019, a second accommodation reported to [REDACTED] that there is “an alarming situation with [REDACTED] reservations”. Several guests who had booked through [REDACTED] were contacted by telephone with the request to provide their credit card details. This accommodation also asked the [REDACTED] to investigate.

E-mail of 20 January 2019 11:35 hours

“Good morning [...]

We have an alarming situation with [REDACTED] reservations. The last couple of days, we have guests reserved through [REDACTED], contacting us to inform us that someone from our in-house reservations department called them to get their credit card details for their reservations. The person who calls the guests knows their reservation details (arrival/departure etc.). Attached and below you can find more details about this matter.

We have already changed the [REDACTED] password as well as my own password.

Can you please look into this?

Thank you,

[...]

It is [REDACTED]'s policy that suspicions and reports of incidents must be forwarded immediately to [REDACTED]'s Security Team.¹²

[REDACTED]'s [REDACTED] who had been informed by the accommodations of fraudulent acts by an unknown third party informed [REDACTED]'s Security Team on 31 January 2019.

On 4 February 2019, [REDACTED]'s Security Team completed its initial investigation and concluded that [REDACTED]'s Privacy Team should be informed. The findings of the investigation by the Security Team are recorded in the aforementioned Security Incident Summary Report dated 28 February 2019.¹³

This investigation by the Security Team revealed that 40 accommodations in the United Arab Emirates had been the victim of social engineering fraud, whereby the personal data of 4,109 data subjects may have been compromised. An unknown third party pretended to be an employee of [REDACTED] on the telephone in order to obtain the username, password and two-factor authentication code (2FA) of the accommodation.

¹² See file document 15, Reply to request for information with regard to internal policy documents on data breaches.

¹³ File document 9, [REDACTED]'s replies to requests for information, Appendix 5.



Date
10 December 2020

Our reference
[REDACTED]

This information allowed the third party to log onto [REDACTED]'s Extranet which contains reservation details of guests. The Security Team has determined that the starting date of the security incident was 19 December 2018. The data subjects were from Europe (including the United Kingdom, France, Ireland, Switzerland, Belgium, the Netherlands) as well as from other parts of the world (including South Africa, America, Canada and Bahrain).

The personal data concerned included first name, surname, address, telephone number, check-in and check-out date, total price, reservation number, price per night, any correspondence between the accommodation and, with regard to 283 data subjects, their guest and credit card details including the card verification code of 97 of these data subjects.

On 4 February 2019, the Security Team informed [REDACTED]'s Privacy Team of the outcome of the investigation. On 4 February 2019, [REDACTED] also informed all data subjects.¹⁴

On 6 February 2019, [REDACTED]'s Privacy Team determined that there was a personal data breach that must be reported to the AP.

On 7 February 2019, [REDACTED] notified the AP of a personal data breach as defined in Article 33(1) of the GDPR.¹⁵

3.4.3 Assessment

Article 33(1) of the GDPR provides 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 (...), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Before the notification is made, therefore, the controller must first assess whether there is a personal data breach. It must then be assessed whether the infringement poses a risk to the rights and freedoms of natural persons.

A personal data breach

As ascertained by the AP in paragraph 3.4.2, an unknown third party accessed [REDACTED]'s Extranet and thereby gained unauthorised access to the data processed by [REDACTED] concerning reservations of guests at accommodations. [REDACTED] also does not dispute the existence of a personal data breach. As a result, the AP ascertains that there is a personal data breach as defined in Article 4(12) of the GDPR.

Risk to the rights and freedoms of natural persons

Following the unauthorised acquisition of the aforementioned personal data, the unknown third party then attempted to use this personal data to obtain credit card details of guests who had booked via [REDACTED]'s online platform. As a result, the AP not only ascertains that the personal data breach is likely to

¹⁴ Notification form and views expressed, marginal 4.4(d).

¹⁵ File document 1: notification of a personal data breach 7-2-2019, p 5.



Date
10 December 2020

Our reference
[REDACTED]

jeopardise the rights and freedoms of natural persons, but also that this risk has materialised since the unknown third party contacted many, if not hundreds, of data subjects to try to swindle credit card data on improper grounds. As a result of the confidentiality breach of personal data, there was a risk not only of financial damage but also of identity fraud or any other harm. The AP therefore ascertains that the personal data breach posed a risk to the rights and freedoms of natural persons.

Notification to the competent supervisory authority in accordance with Article 55

In paragraph 3.3 it is established that [REDACTED] is the controller. In paragraph 3.1, the AP established that it is competent to act as the lead supervisory authority, in accordance with Article 56 of the GDPR, since [REDACTED]'s main establishment is in Amsterdam. [REDACTED] notified the AP of the breach on 7 January 2019. In doing so, [REDACTED] made the notification to the competent authority in this case, in accordance with Article 55 of the GDPR.

Notification not later than 72 hours after the controller becomes aware of a personal data breach

The Guidelines on Personal Data Breach Notification under Regulation 2016/679¹⁶ (hereinafter: Guidelines), drawn up by the Article 29 Data Protection Working Party (hereinafter: WP29), explain the notification requirements of the GDPR and provide guidance on how to proceed in the event of various types of breaches.

The precise moment when a controller can be considered to be aware of a particular breach depends on the circumstances of the particular breach. According to the WP29, a controller should be deemed to have become aware of a personal data breach when it has a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised.

In the opinion of the AP, [REDACTED] was aware of the personal data breach in any case on 13 January 2019 and finds as follows.

On 9 January 2019, [REDACTED]'s [REDACTED] received an initial signal, via an e-mail from a [REDACTED] in the United Arab Emirates (accommodation I), that both the data subject and the [REDACTED] suspected there had been a personal data breach. The data subject was contacted by e-mail on 8 January 2019 by an unknown third party who was familiar with the reservation made through [REDACTED]'s platform and who, on the basis of this reservation information, was trying to obtain additional personal details in order to supposedly arrange payment for an overnight stay. The e-mail of 8 January 2019, which is included in the file, also attached a PDF document with the booking details. Incidentally, this PDF file has not been submitted by [REDACTED] and has therefore not been included in the file.

In the opinion of the AP, the aforementioned incident should have been forwarded by (the [REDACTED] of) [REDACTED] to its Security Team for further investigation since the e-mail in question contained the precise booking details of the data subject and it had also been established that the booking had been made via [REDACTED]'s platform. This is even more applicable as the [REDACTED] had already come to the conclusion

¹⁶ Guidelines on Personal Data Breach Notification under Regulation 2016/679, Article 29 Data Protection Working Party, last revised and adopted on 6 February 2018, 18/NL WP250rev.01.



Date
10 December 2020

Our reference
[REDACTED]

that there was a security incident and had already made an initial assessment on the basis of the information at his disposal. This is also evident from the subject of the e-mail mentioned by the accommodation manager: "[External] Fraud / Leaked Guest Information / URGENT". The Security Team could have started an exploratory investigation at this time.

On 13 January 2019, (the same [REDACTED] of) [REDACTED] received a second message from the aforementioned [REDACTED]. The data subject in question had been asked for his personal details by telephone by someone posing as an employee of [REDACTED] who was aware of the reservation made by the data subject through the [REDACTED] platform. In his e-mail to [REDACTED]'s [REDACTED], the accommodation manager expressly stated that he considered the incident to be equivalent to the previous incident and again believed that there must be a data breach on [REDACTED]'s side.

The AP is of the opinion that [REDACTED] is deemed to have knowledge of the personal data breach at least on 13 January 2019, because the above information gave [REDACTED] a reasonable degree of certainty that a security incident had occurred that had led to personal data processed by [REDACTED] being compromised. In fact, the accommodation manager of the [REDACTED] had already concluded that there must have been a security incident involving the Extranet whereby personal data of guests had been compromised.

Given the alarming situation, [REDACTED] should have immediately referred the incident to [REDACTED]'s Security Team so that the extent of the breach could be investigated, but instead [REDACTED] failed to do so until 31 January 2019.

On the basis of the above, the deadline of 72 hours for reporting a breach to the AP, as stipulated in Article 33(1) of the GDPR, started on 13 January 2019. As a result, [REDACTED] should have notified the AP of the personal data breach by 16 January 2019 at the latest. It is an established fact that [REDACTED] only made this notification on 7 February 2019, i.e. 22 days too late.

The same applies if 20 January 2019 should be adopted as the starting date, which is the date on which another [REDACTED] (accommodation II) in the United Arab Emirates reported similar incidents to [REDACTED]'s [REDACTED] as accommodation I. In this e-mail, the subject is also highlighted in capital letters: **SECURITY BREACH**. In this case, the personal data breach would have been notified to the supervisory authority 15 days too late.

3.4.4 Views expressed by [REDACTED] and response of the AP

Breach notification

[REDACTED] has primarily argued in its views that no infringement occurred since it only became aware of the breach on 4 February 2019 upon completion of its internal investigation, after which the breach was notified in a timely manner and without undue delay within 72 hours of [REDACTED] becoming aware of it. This, according to [REDACTED], is in conformity with Article 33(1) of the GDPR.



Date

10 December 2020

Our reference

[REDACTED]

The AP does not agree with this viewpoint. As can be seen from the above, the AP has established that [REDACTED] became aware of the breach on 13 January 2019. It follows from this that [REDACTED] did not notify the personal data breach in accordance with the provisions of Article 33(1) of the GDPR.

Reports by accommodations

With regard to the message from accommodation I on 9 January 2019, [REDACTED] argued when expressing its views that at the time [REDACTED]'s [REDACTED] considered that there was no reason to forward the report to [REDACTED]'s Security Team, because the data subject in question had been contacted by e-mail. [REDACTED] states that e-mail addresses in the Extranet are hashed and cannot be extracted. [REDACTED] further argues that the accommodation in question and [REDACTED]'s [REDACTED] jointly concluded that "it was probably not an incident at [REDACTED]".

With regard to the latter, the AP notes that, in addition to the fact that the views expressed by [REDACTED] do not substantiate this, it is established that [REDACTED]'s [REDACTED] did not act in accordance with [REDACTED]'s own protocol, which stipulates that any suspicion of an incident must be immediately forwarded to [REDACTED]'s Security Team. The AP is of the opinion that, despite the fact that e-mail addresses are hashed in the Extranet, the aforementioned incident should have been forwarded by [REDACTED] to the Security Team. After all, the fact that the e-mail in question contained the exact booking details of the data subject and the fact that the booking was made via [REDACTED]'s platform should have alerted [REDACTED]'s [REDACTED] and prompted him to take further action.

With regard to the incident of 13 January 2019, [REDACTED] argued that the [REDACTED] in question did not see any direct similarities with the previous incident, which meant that it could not be established with a reasonable degree of certainty that a security incident had occurred at [REDACTED].

However, the AP is of the opinion that the fact that the (accommodation manager of the) [REDACTED] had already considered that there was an equivalent incident and that the security incident must be in relation to the Extranet, for which [REDACTED] is the controller, means that at that time [REDACTED] did know with a reasonable degree of certainty - and therefore had become aware - that a personal data breach had occurred. Again in this case the precise booking details of the data subject were known to an unknown third party who falsely pretended to be an employee of [REDACTED]. At this point, [REDACTED] had a reasonable degree of certainty with regard to the security incident in which personal data had been compromised. There was a high degree of certainty that this data had been obtained from a platform used by [REDACTED] for its business purposes, since the e-mail correspondence showed that both the [REDACTED] and the data subject in question could rule out the possibility that a security incident had occurred on their side.

Breach of internal reporting obligation

[REDACTED] has further argued that the fact that the procedure for reporting security incidents, where security incidents must be reported by the [REDACTED] to the [REDACTED] Security Team via the Partner Portal, was infringed by the accommodation in question¹⁷. According to [REDACTED], the breach of that obligation to notify and the fact that [REDACTED]'s [REDACTED] did not immediately forward the incident should not be

¹⁷ In this case, the accommodation in the United Arab Emirates.



Date

10 December 2020

Our reference

[REDACTED]

held against [REDACTED] as a company. [REDACTED] also referred to a decision of the Hungarian privacy supervisory authority, which found that negligence on the part of only one part of an organisation could not be invoked against the whole organisation if appropriate measures had been taken.¹⁸

The AP states that it is of paramount importance that [REDACTED], as the controller, has an obligation to investigate any possible personal data security breach in response to every alarming signal in order to act in a timely manner and in accordance with the provisions of the GDPR. According to the AP, this is separate from any private law agreements that [REDACTED] may have made in that respect with a third party, such as, in the present case, the [REDACTED] in question. Paragraph 5.1 of the 'Data Incident Response Policy' submitted by [REDACTED] also shows that all suspicions of incidents, even if reported to [REDACTED] by third party service providers such as [REDACTED], must be immediately forwarded to [REDACTED]'s Security Team:

"Prompt Reporting

All (suspected) Data Incidents must immediately be reported to the [REDACTED] security team ("Security"). This includes Data Incidents notified to [REDACTED] from any third party service providers or business partners or other individuals. (...)".

Although various data incidents were reported by the accommodations to the [REDACTED] of [REDACTED] on 9, 13 and 20 January 2019, this did not lead to the required reporting of these incidents to the Security Team, as set out in [REDACTED]'s own procedures. While [REDACTED]'s [REDACTED] was already aware of the breach on 13 January 2019, the Security Team was only informed on 31 January 2019.

Insofar as [REDACTED] has sought to rely on the principle of equality by referring to the decision of the Hungarian supervisory authority, the AP notes that the case in question is not only a breach of an entirely different nature, namely a breach of the confidentiality of personal data by the same organisational unit (of a public body) and not a case of social engineering involving a form of fraud, but also that the AP understands this decision of the supervisory authority differently than as outlined by [REDACTED]. The fact that the notification of a breach, as defined in Article 33(1) of the GDPR, was too late in that case because an employee forwarded it too late, was held against the organisation in question by the Hungarian supervisory authority, contrary to what [REDACTED] suggests.

Risk to privacy

[REDACTED] also argued that the investigation report wrongly assumed that there was a risk to privacy without analysing the security measures implemented by [REDACTED] with a view to protecting privacy and removing adverse consequences, and gave a number of examples.¹⁹

¹⁸ Fining Decision of the Hungarian National Authority for Data Protection and Freedom of Information dated 21 May 2019, NAIH/2019/3854.

¹⁹ The examples mentioned: if a data breach occurs, this is generally limited to contact details, without e-mail addresses, and reservation dates; credit card details are stored in accordance with PCI DSS standards; customers are informed about social engineering and other forms of fraud; the data subjects were immediately informed and given advice after the data breach was detected and [REDACTED] has indicated that it will compensate all damage suffered.



Date

10 December 2020

Our reference

[REDACTED]

The AP does not agree with the latter viewpoint of [REDACTED]. At such time as personal data are in the hands of and are accessed by an unauthorised person, as in this case, then there is already a risk to the rights and freedoms of natural persons. This risk has also manifested itself in this case, where data subjects were approached by an unknown third party who unlawfully possessed the personal data of the data subjects. The fact that [REDACTED] subsequently undertook to provide compensation for any financial damage does not alter the fact that the personal data ended up in the wrong hands. This does not eliminate the risk of any consequences of the breach.

Notification within 72 hours

[REDACTED] has also argued that it is not always possible to make a notification within 72 hours, as referred to in Article 33(1) of the GDPR. It can take weeks or months for specialist security teams to connect data points and reach the conclusion that a factual pattern is indeed a data breach that should be notified. Furthermore, it would be wrong and inconsistent with the GDPR for the AP to expect [REDACTED] to generally only need three days to conduct an investigation and become aware of a personal data breach. In addition, according to [REDACTED], the WP29 explicitly mentions in its Guidelines that it may take some time for a controller to establish the extent of the breaches and be able to prepare a meaningful notification combining several very similar breaches rather than reporting each breach separately. Finally, [REDACTED] argued that the investigation report wrongly concluded that [REDACTED] had failed to give a valid reason for the (alleged) infringement of the 72-hour deadline. The notification of 7 February 2019 gives clear reasons, based on [REDACTED]'s in-depth investigation, reiterating that [REDACTED]'s primary position is that the notification was made within 72 hours of it becoming aware of the personal data breach.

The AP considers as follows in this regard.

The AP agrees with the view that an investigation into the scope and precise merits of a breach can take longer than 72 hours. As it is not always possible to have all the necessary information about a breach in order to make a notification that meets all the requirements laid down in Article 33(3) of the GDPR, the option of making a notification in phases has been included in the GDPR. This option is laid down in Article 33(4) of the GDPR. The notification of the breach, however, must take place within the statutory deadline of 72 hours, in accordance with Article 33(1) of the GDPR. As noted in paragraph 3.3.3, it must be considered that [REDACTED] became aware of the personal data breach on 13 January 2019. The fact that the breach should have been notified, in accordance with Article 33(1) of the GDPR, was also clear at that time. In this case, [REDACTED] waited too long before making the notification required by Article 33(1) of the GDPR. The thorough investigation to which [REDACTED] refers in no way justifies the delay of the aforementioned (initial) notification, which therefore constitutes an unreasonable delay within the meaning of Article 33(1) of the GDPR.

Meaningful notification



Date
10 December 2020

Our reference
[REDACTED]

With regard to the allegations made by [REDACTED] concerning the preparation of a meaningful notification combining several similar breaches, the AP considers that the issue at stake in the present case is that [REDACTED] was aware of the breach as early as 13 January 2019 and should have made the notification - initial or otherwise - in a timely manner. The AP does not consider it relevant - in view of what has been considered in paragraph 3.4.3 above - that there are several similar breaches here which, according to [REDACTED], could be packaged into a single meaningful notification.

Justification of the delayed notification

[REDACTED] has argued that there are no instructions that specify the arguments for justifying a delayed notification except the Guidelines and that the AP cannot apply a new standard retroactively. In addition, the AP could have asked for a clarification of the delay.

The AP considers that there is no question of applying a new standard retroactively. The rules set out in the GDPR are clear on this point: 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. The Guidelines, in the opinion of the AP, provide guidance on how to comply with the obligation to notify breaches as laid down in the GDPR and cannot therefore be considered as a new standard. For that matter, it is at all times up to the controller to provide adequate reasoning for a notification that cannot be made in a timely manner.

Practical implications of the opinion of the AP

In the views expressed by [REDACTED], it also stated its concerns about the practical implications of the opinion of the AP in the investigation report.²⁰ According to [REDACTED], the strict interpretation contained therein means that all potential security incidents where there is a risk of personal data being compromised must be reported within 72 hours and that the Security Team must investigate any complaint received by [REDACTED], irrespective of the manner and content of the complaint. This would impose an unreasonable and unrealistic administrative burden as well as an unreasonable and unrealistic financial burden.²¹ [REDACTED]

[REDACTED]. If all individual complaints were to be investigated immediately, as advocated by the AP, it would need considerably more manpower than at present. According to [REDACTED], such unreasonable organisational measures, with their disproportionate costs of implementation, run counter to the concept of a duty to protect personal data as defined in Article 32 of the GDPR.

The AP states first and foremost that the GDPR stipulates the obligations that [REDACTED] has to meet as a controller. Article 32 of the GDPR requires a data controller to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk: the ability to detect, address

²⁰ Paragraph 5 of the views expressed by [REDACTED].

²¹ [REDACTED]
[REDACTED].



Date

10 December 2020

Our reference

[REDACTED]

and report a breach in a timely manner should be considered an essential part of these measures.²² According to the AP, it does not follow from the investigation report that every potential security incident should be reported and every complaint received by [REDACTED] should be investigated by the Security Team. As soon as a controller becomes aware of a security incident or has been informed of a possible breach by another source, the controller must investigate whether the breach is subject to notification.²³ It is apparent that [REDACTED] has organised its Data Incident Response Policy in such a way that suspicions and reports of alleged security incidents must be immediately forwarded to the Security Team for assessment. In the opinion of the AP, the fact that this did not occur in this case is at the expense and risk of [REDACTED]. In this context, the AP once again draws attention to the fact that, on the basis of the various reports from the accommodations, there is virtually no other conclusion that can be reached than that this was a substantial breach that was subject to notification.

Manifest clerical error in the report

[REDACTED] has argued that paragraph 26 of the investigation report erroneously mentions 2 February 2019 as the date on which [REDACTED]'s Security Team recorded its findings, but that this date is not mentioned anywhere else in the documents. The AP has assumed that this is a manifest clerical error, since the documents do not provide any basis for the fact that the Security Team presented its findings on 2 February 2019.

For the sake of completeness

Although this is not under discussion in this case, [REDACTED] has indicated in its expressed views that it attaches considerable importance to data security and immediate action being taken with regard to data breaches. [REDACTED] considers that it more than meets, and even exceeds, the expectations set out in Article 34 of the GDPR by informing data subjects about data breaches, even where there is unlikely to be a significant risk to the rights and freedoms of data subjects. The AP welcomes such actions but stresses that this does not release [REDACTED] from the other obligations laid down in the GDPR, such as the notification obligation in Article 33(1) of the GDPR.

3.4.5 Conclusion

In view of the above, the AP is of the opinion that [REDACTED] infringed Article 33(1) of the GDPR from 16 January 2019 to 6 February 2019, since [REDACTED] failed to report the personal data breach to the AP in a timely manner and without undue delay.

²² See Guidelines, p. 14/15.

²³ See the WP29 Guidelines for more details.



Date

10 December 2020

Our reference

[REDACTED]

4. Fine

4.1 Introduction

As a result of the breach identified above, the AP makes use of its power to impose a fine on [REDACTED] under Article 58(2)(i) and Article 83(4) of the GDPR, read in conjunction with Article 14(3) of the General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene verordening gegevensbescherming*). The AP applies the 2019 Fining Policy Rules for this purpose (hereinafter: Fining Policy Rules).²⁴

In the following, the AP will first briefly set out the system of fines, followed by the reasons for the amount of the fine in the present case.

4.2 Fining Policy Rules of the Dutch Data Protection Authority 2019 (hereinafter: 2019 Fining Policy Rules)

Pursuant to Article 58(2), preamble and under (i) and Article 83(4) of the GDPR, read in conjunction with Article 14(3) of the General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene verordening gegevensbescherming*), the AP is authorised to impose an administrative fine on [REDACTED] up to € 10,000,000 or up to 2% of the total worldwide annual sales volume in the preceding business year, whichever figure is higher, in the event of an infringement of Article 33(1) of the GDPR.

The AP has adopted Fining Policy Rules for the interpretation of the aforementioned power to impose an administrative fine, including the determination of the amount thereof.²⁵

Pursuant to Article 2(2.1) of the 2019 Fining Policy Rules, the provisions in respect of which the AP may impose an administrative fine of up to € 10,000,000 or, in the case of a company, up to 2% of its total worldwide annual sales volume in the preceding business year, whichever figure is the higher, are classified in Appendix 1 into categories I, II or III.

In Appendix 1, Article 33(1) of the GDPR is classified into category III.

Pursuant to Article 2(2.3) of the Fining Policy Rules, the AP sets the basic fine for category III offences within the following fine range: € 300,000 and € 750,000 and a basic fine of € 525,000.

Pursuant to Article 6, the AP determines the amount of the fine by adjusting the amount of the basic fine either upwards (up to the maximum in the fine range associated with a breach category) or downwards (to the minimum in that range). The basic fine will be increased or decreased depending on the extent to which the factors referred to in Article 7 give cause to do so.

²⁴ Government Gazette 2019, 14586, 14 March 2019.

²⁵ Government Gazette 2019, 14586, 14 March 2019.



Date

10 December 2020

Our reference

[REDACTED]

Pursuant to Article 7, without prejudice to Articles 3:4 and 5:6 of the General Administrative Law Act (*Algemene wet bestuursrecht*), the AP takes into account the factors derived from Article 83(2) of the GDPR in the Policy Rules referred to under (a) to (k):

- 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 [...] to mitigate the damage suffered by data subjects;
- d. the degree of responsibility of the controller [...] taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
- e. any relevant previous infringements by the controller [...];
- 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 [...] notified the infringement;
- i. where measures referred to in Article 58(2) have previously been ordered against the controller [...] 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.

Pursuant to Article 9 of the 2019 Fining Policy Rules, the AP is obliged to take the financial circumstances of the offender into account when setting the fine where appropriate. In the event of reduced or insufficient capacity of the offender, the AP may further moderate the fine to be imposed if, after application of Article 8.1 of the Fining Policy Rules, setting a fine within the fine range of the next lower category would, in its opinion, nevertheless result in a disproportionately high fine.

4.3 Amount of the fine

4.3.1. Nature, gravity and duration of the breach

Pursuant to Article 7, preamble and under a, of the Fining Policy Rules, the AP shall take the nature, gravity and duration of the breach into account. In assessing this, the AP shall take into account the nature, scope or purpose of the processing as well as the number of data subjects affected and the extent of the damage suffered by them.

The protection of natural persons with regard to the processing of personal data is a fundamental right. Pursuant to Article 8(1) of the Charter of Fundamental Rights of the European Union (*Handvest van de grondrechten van de Europese Unie*) and Article 16(1) of the Treaty on the Functioning of the European Union (*Verdrag betreffende de werking van de Europese Unie*), everyone has the right to the protection of their personal data. The principles and rules relating to the protection of natural persons with regard to the processing of



Date

10 December 2020

Our reference

[REDACTED]

their personal data must comply with their fundamental rights and freedoms, in particular their right to the protection of personal data. The purpose of the GDPR is to contribute to the creation of an area of freedom, security and justice and an economic union, as well as to economic and social progress, the strengthening and convergence of economies within the internal market and the well-being of natural persons. The processing of personal data must be designed to serve mankind. The right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and weighed against other fundamental rights in accordance with the principle of proportionality. Any processing of personal data must be proper and lawful. Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed. Personal data must be processed in a manner that ensures appropriate security and confidentiality of that data, including to prevent unauthorised access to or use of personal data and the equipment used for processing.

Notification of breaches should be seen as a means of improving compliance with the rules on the protection of personal data. If a personal data breach takes place or has taken place, it may result in bodily, material or immaterial harm to natural persons or any other economic or social harm to the person concerned. Therefore, as soon as the controller becomes aware of a personal data breach, it should notify the supervisory authority of the personal data breach without undue delay and, if possible, within 72 hours. This will enable the supervisory authority to carry out its tasks and powers properly, as laid down in the GDPR.

[REDACTED] not only failed to notify the personal data breach without delay, it also failed to do so on several occasions, i.e. on 9, 13 and 20 January 2019, when immediate action should have been expected and which resulted in a (very) undue delay in notifying the AP. Furthermore, instead of making a notification in phases, it has been shown that [REDACTED] deliberately chose to conduct an in-depth investigation before making the required notification to the supervisory authority. This is not in line with the rules laid down in the GDPR.

The investigation carried out by [REDACTED]'s Security Team revealed that 4,109 people may have been affected. These were hotel guests, who had booked hotel accommodation at 40 different accommodations through the [REDACTED] platform. By committing social engineering fraud, unauthorised third parties acquired credit card details as well as name and address details and details of hotel reservations. These are sensitive data which, in the hands of unauthorised persons, can lead to financial loss or other harm.

In view of the nature of the personal data, the amount of the personal data, the number of data subjects affected, the duration of the infringement and the importance of notifying the supervisory authority in a timely manner within 72 hours, the AP considers that this is a serious infringement but sees no reason to increase or decrease the basic amount of the fine.

4.3.2 Intentional or negligent character of the infringement(culpability)

Pursuant to Article 5:46(2) of the General Administrative Law Act (*Algemene wet bestuursrecht*), when imposing an administrative fine, the AP should take into account the extent to which the offender is



Date
10 December 2020

Our reference
[REDACTED]

culpable. Pursuant to Article 7(b) of the 2019 Fining Policy Rules, the AP should take into account the intentional or negligent character of the infringement.

Article 33(1) of the GDPR stipulates that a personal data breach must be notified without undue delay and, where feasible, not later than 72 hours after the controller has become aware of it. The obligation to notify has been in effect in the Netherlands since 1 January 2016, when this standard was introduced in the Personal Data Protection Act (*Wet bescherming persoonsgegevens*).²⁶

Given that a party to which a certain standard applies, such as [REDACTED] in this case, is deemed to have knowledge of the applicable laws and regulations, the AP takes the view that market parties have their own responsibility to comply with the law.²⁷

The AP has also provided market parties with ample information about the applicable laws and regulations, so that it can be assumed that [REDACTED] was familiar with them. In addition, the notification obligation with regard to data breaches has been widely reported in the media.

In the opinion of AP it should have been sufficiently clear to [REDACTED] from the legal framework set out above in conjunction with the applicable WP29 Guidelines, which [REDACTED] could have taken note of prior to the breach, that it should have notified the AP of the breach in a timely manner and without undue delay, but in any event no later than 72 hours after 13 January 2019. In addition, the notification to the AP could have been made on a conditional basis and the notification could have been supplemented afterwards. This option is expressly provided for in the GDPR.

If [REDACTED] had any doubts about the scope of the notification obligation, a professional and multinational market operator such as [REDACTED] can be expected to properly obtain information about the restrictions to which its conduct is subject, also according to established case law, in order to adjust its conduct to the scope of that obligation from the outset.²⁸

In the opinion of the AP, as an independent party having rights and obligations, [REDACTED] cannot exculpate itself from the fact that a [REDACTED] acted contrary to [REDACTED]'s own protocol, which stipulates that any suspicion of an incident must be immediately forwarded to the Security Team for assessment. This is attributable to [REDACTED].

[REDACTED] reported the breach 22 days too late. The AP considers this to be culpable. However, the AP sees no reason to increase or decrease the basic amount of the fine under Article 7(b) of the 2019 Fining Policy Rules.

4.3.3 Actions taken to mitigate the damage suffered

Pursuant to Article 7(c) of the 2019 Fining Policy Rules, the AP is required to take into account any action taken by the controller to mitigate the damage suffered by the data subjects.

²⁶ Article 34a(1) of the Personal Data Protection Act (*Wet bescherming persoonsgegevens*).

²⁷ Cf. Trade and Industry Appeals Tribunal 25 June 2013, ECLI:NL:CBB:2013:4, grounds 2.3, Trade and Industry Appeals Tribunal 25 January 2017, ECLI:NL:CBB:2017:14, grounds 5.2, Trade and Industry Appeals Tribunal 8 March 2017, ECLI:NL:CBB:2017:91, grounds 6.

²⁸ Cf. Trade and Industry Appeals Tribunal 22 February 2012, ECLI:NL:CBB:2012:BV6713, grounds 4.3, Trade and Industry Appeals Tribunal 19 September 2016, ECLI:NL:CBB:2016:290, grounds 8.6., Trade and Industry Appeals Tribunal 19 September 2016, ECLI:NL:CBB:2016:372, grounds 6.3.



Date

10 December 2020

Our reference

[REDACTED]

In the views expressed by [REDACTED], it has put forward several specific remedial actions in order to limit possible damage to the data subjects. For example, [REDACTED] has informed and advised the data subjects about taking measures to reduce the damage. [REDACTED] has also declared itself willing to compensate any damages (suffered or to be suffered) by the data subjects. Finally, [REDACTED] immediately informed the affected accommodations and placed warnings on the [REDACTED] platform.

The AP is of the opinion that, although [REDACTED] failed to report the breach to the supervisory authority in a timely manner, it is to [REDACTED]'s credit that it has taken the above measures and declared itself willing to compensate any damages. The fact that [REDACTED] ultimately acted expeditiously in this respect, which most likely limited the detrimental impact on the data subjects, is taken into account by the AP in determining the level of the fine.

In view of the actions taken by [REDACTED] to mitigate the damage of the data subjects resulting from the breach, the AP sees reason to reduce the basic amount of the fine by € 50,000 in accordance with Article 7(c) of the 2019 Fining Policy Rules.

4.3.4 Other circumstances

Furthermore, the AP does not see any reason to increase or decrease the basic amount of the fine on the basis of other circumstances, as referred to in Article 7 of the 2019 Fining Policy Rules, insofar as applicable in the present case.

In view of the factors mentioned in Article 7 of the GDPR, the AP sets the amount of the fine for the infringement of Article 33(1) of the GDPR at € 475,000.

4.3.5 Viewpoint of [REDACTED] and response of the AP

With regard to the imposition of an administrative fine, in the views expressed by [REDACTED] it primarily argued that the imposition of an administrative fine would not be proportionate. In this respect, [REDACTED] referred to fines imposed by the Lithuanian, Hungarian and Hamburg authorities for infringements of Article 33(1) of the GDPR.²⁹ [REDACTED] takes the viewpoint that, within the framework of the idea of harmonisation, the same fines should be imposed for similar offences within Europe.

At present, no common principles for the calculation of fines have been agreed at European level. Consequently, the AP independently applies its own Fining Policy Rules for the calculation of fines. In addition, the AP is assessing this case on its own merits and thus according to the specific facts and circumstances of the case. It goes without saying that these are different in each case and therefore not comparable with each other. Finally, the fine decisions of other privacy supervisory authorities as expounded by [REDACTED] in its views, were not reached on the basis of the consistency mechanism, as laid down in Article 60 of the GDPR, and the AP is therefore not bound by those decisions and is not bound to impose a fine of an equal amount in the present case.

²⁹ Paragraph 9.2(a) of the views expressed by [REDACTED].



Date
10 December 2020

Our reference
[REDACTED]

[REDACTED] also argued that, in the absence of clear guidelines from the AP and the European Data Protection Board (*Europees Comité voor Gegevensbescherming*) in respect of the reasons for a delay in reporting a data breach, the imposition of an administrative fine would violate the *lex certa* principle.

The AP also does not agree with this viewpoint of [REDACTED] and refers to what has been considered in paragraphs 3.4.4 and 4.3.2 of this decision.

Finally, [REDACTED] argued as a second alternative that if the AP nevertheless decides to impose a fine, it should be reduced to the lowest fine in category II in accordance with Article 6 in conjunction with Article 8.1 of the Fine Policy Rules.

With regard to the nature, gravity and duration of the infringement, [REDACTED] has briefly argued that the preventive and corrective measures taken by [REDACTED] have limited both the number of people affected and the extent of the damage.

However, with reference to paragraph 4.3.1, the AP sees no reason to refrain from imposing an administrative fine or to reduce the amount of the fine.

With regard to the intentional or negligent character of the infringement, [REDACTED] has argued that the breach is not the result of any intention or negligence on the part of [REDACTED] and refers to the technical and organisational measures taken to prevent social engineering incidents and to limit the consequences.

The AP rejects this viewpoint. As stated in paragraph 4.3.2, the AP is of the opinion that negligence is attributable to [REDACTED]. The AP sees no reason to increase or decrease the basic amount of the fine.

With regard to the measures taken to limit the damage, [REDACTED] argues that the technical and organisational measures it has taken are appropriate and may even exceed the requirements of the GDPR.

As discussed in paragraph 4.3.3 above, the AP considers this as a reason to reduce the basic amount of the fine.

With regard to the degree of responsibility given the technical and organisational measures taken by [REDACTED], in accordance with Articles 25 and 32 of the GDPR, [REDACTED] has argued that its systems and organisation are designed in such a way that the principles of data protection can be effectively implemented, reiterating that, given the measures taken and the nature of the incident, [REDACTED] cannot be held liable for the data breach and the alleged infringement.

The AP does not share this viewpoint. A professional party such as [REDACTED] may be expected to be fully aware of and comply with the standards applicable to it, also given the nature and extent of the processing. As previously considered in paragraph 4.3.2 of this decision, [REDACTED] is fully responsible for the infringement. Consequently, the AP does not see any reason to reduce the fine in this case either.



Date

10 December 2020

Our reference

[REDACTED]

With regard to previous relevant breaches of the GDPR, [REDACTED] has argued that it had not previously received a notice from the AP regarding alleged breaches of Article 33(1) of the GDPR.

The AP fails to understand why this viewpoint of [REDACTED] should lead to a reduction in the basic amount of the fine. The fact that the AP has not previously sent a notice to [REDACTED] regarding an identical offence does not lead to a reduction in the amount of the fine.

[REDACTED]
[REDACTED]
[REDACTED].

With regard to the cooperation between [REDACTED] and the AP to remedy the alleged infringement and mitigate its possible adverse effects, [REDACTED] has argued that it fully cooperated with the AP by answering all questions in a timely manner and that if the AP had asked for an explanation for the delay in the notification then this explanation would have been given.

The AP sees no reason to reduce the amount of the fine in this regard. The AP considers that [REDACTED]'s cooperation has not gone beyond its legal obligation to comply with Article 33(1) of the GDPR. [REDACTED] did not cooperate with the AP in any special way.

With regard to the other factors, [REDACTED] has briefly argued that the personal data does not fall under special categories of personal data or belong to a vulnerable group of persons, that [REDACTED] has been fully transparent to the data subjects and that it notified the AP of the data breach itself. Finally, [REDACTED] has argued that if it had notified the AP earlier, this would not have led to any other action on [REDACTED]'s part or to further reduction of the risks to the privacy of the data subjects. According to [REDACTED], none of the data subjects suffered any damage at all as a result of the timing of the notification.

Again, the AP does not agree with the views expressed by [REDACTED]. Despite the fact that, as far as we know, the breach did not affect any special personal data, that [REDACTED] independently informed those concerned and that the (financial) consequences were limited for the data subjects, the AP sees no reason to further reduce the amount of the fine because of the seriousness of the infringement and [REDACTED]'s culpability. The AP refers to paragraphs 4.3.1 and 4.3.2 for its reasoning.

4.3.6 Proportionality and maximum legal fine

Finally, on the basis of the principle of proportionality laid down in Articles 3:4 and 5:46 of the General Administrative Law Act (*Algemene wet bestuursrecht*), the AP assesses whether the application of its policy for determining the level of the fine would lead to a disproportionate outcome in view of the circumstances of the specific case. The application of the principle of proportionality, according to the 2019 Fining Policy Rules, means that the AP must take into account the financial circumstances of the offender where appropriate when setting the fine.



Date

10 December 2020

Our reference

[REDACTED]

In light of all the above considerations, the AP considers that the level of the fine to be imposed does not lead to a disproportionate outcome. In addition, this decision has been taken by means of the consistency mechanism provided for in the GDPR. The other European supervisory authorities involved have endorsed the assessment of the AP.

Given its financial position, the AP sees no reason to assume that [REDACTED] would not be able to bear a fine of € 475,000.

4.4 Conclusion

The AP sets the total amount of the fine at € 475,000.

5. Operative part

Fine

AP imposes an administrative fine of **€ 475,000** (in words: four hundred and seventy-five thousand euros) on [REDACTED] for the infringement of Article 33(1) of the GDPR.³⁰

Yours sincerely,
Dutch Data Protection Authority

[REDACTED]
[REDACTED]

Remedy clause

If you do not agree with this decision, you can submit a notice of objection, either electronically or on paper, to the Dutch Data Protection Authority within six weeks of the date on which the decision was sent digitally or on paper.

The submission of an objection suspends the operation of the decision imposing the administrative fine, pursuant to Article 38 of the General Data Protection Regulation (Implementation) Act (*Uitvoeringswet Algemene verordening gegevensbescherming*).

To submit an objection digitally, see www.autoriteitpersoonsgegevens.nl, under the heading Objection to a decision, which is at the bottom of the page under the heading Contact with the Personal Data Authority.

³⁰ The AP will hand over the aforementioned claim to the Central Judicial Collection Agency (*Centraal Justitieel Incassobureau*).



Date

10 December 2020

Our reference

[REDACTED]

The address for the submission of an objection on paper is: Dutch Data Protection Authority, PO Box 93374, 2509 AJ The Hague.

Please include 'Administrative objection' on the envelope and 'Objection' in the subject line of your letter.

At a minimum your notice of objection should include:

- your name and address;
- the date of your objection;
- the reference mentioned in this letter (case number) or a copy of this decision should be attached;
- the reasons why you disagree with this decision;
- your signature.

Summary Final Decision Art 60

Legal obligation

Administrative fine

EDPBI:NL:OSS:D:2020:173

Background information

Date of final decision:	10 December 2020
Date of broadcast:	11 December 2020
LSA:	NL
CSAs:	All SAs
Legal Reference:	Notification of a personal data breach to the supervisory authority (Article 33)
Decision:	Administrative fine
Key words:	Personal data breach, Administrative fine

Summary of the Decision

Origin of the case

On 7 February 2019, the service provider of an online platform notified to the LSA a personal data breach that it had discovered on 10 January 2019. The controller indicated in its notification that an unknown third party had gained access to personal data in the controller's reservation system which are used by the platform's partners to manage the reservations. As a result, the personal data of various data subjects who had made reservations via the controller's platform were compromised.

The LSA commenced an investigation on the controller's compliance with Article 33(1) GDPR.

Findings

During its investigations, the LSA found that the controller had been informed on 8 January 2019 by one of its partners that, following a possible personal data breach in the reservation system, an unknown third party had contacted customers and pretended to be affiliated with the controller, once as employee of the controller and other times as an employee of one of the partner organisations on the platform. The LSA noted that the controller received two similar complaints from the same

provider on 13 January 2019 and 20 January 2019; and that on 20 January 2019, a second partner reported the same type of incident.

The LSA noted that, despite the reports about these several incidents, the controller's entity in charge of the receipt of these incidents did not notify the controller's security team until 31 January 2019. After having conducted investigations, the controller's security team informed the controller's privacy team on 4 February 2019.

In view of the circumstances in which the incidents were reported to the controller by the partners, the LSA found that the controller was deemed to have knowledge of the personal data breach at least on 13 January 2019, as the information given by the partner indicated with a reasonable degree of certainty that personal data had been compromised. As a result, the LSA pointed out that the controller should have notified the LSA of the personal data breach by 16 January 2019 at the latest. It is an established fact that the controller only made this notification on 7 February 2019, i.e. 22 days too late. The same applies if 20 January 2019 should be adopted as the starting date, then the notification was done 15 days too late compared to the deadline of 72-hour set out by Article 33(1) GDPR.

In response to the arguments put forward by the controller, the LSA recalled that the fact, that the delay in notifying the data breach was due to a failure by a single part of the controller's organization to report the incident to the security team in accordance with the controller's internal procedure, is without effect. The LSA also stressed that, by choosing to carry out in-depth investigation instead of a notification in phases, the controller did not comply with the rules laid down in Article 33(3) GDPR.

The controller had informed and advised the data subjects about taking measures to reduce the potential damage. The controller had also declared itself willing to compensate any damages (suffered or to be suffered) by the data subjects. The controller also immediately informed its affected partners and placed warnings on the website.

Decision

According to the 2019 Fining Policy Rules adopted by the LSA, the basic fine for the infringement of Article 33(1) of the GDPR was set at € 525,000. In view of the actions taken by the controller to mitigate the damage of the data subjects resulting from the breach, the LSA decided to reduce the basic amount of the fine by € 50,000 in accordance with Article 7(c) of the 2019 Fining Policy Rules adopted by the LSA. The LSA did not find any reason to increase or decrease the basic amount of the fine on the basis of other circumstances.

In the view of the above, the LSA imposed on the controller an administrative fine of € 475,000 for the infringement of Article 33(1) GDPR.



Norwegian Data Protection Authority

[REDACTED]

*Unntatt offentlighet:
Offl. § 13, jf. personopplysningsloven §
24 første ledd 2. punktum*

Your reference

Click here to enter text. Our reference

Our reference

20/02345-11

Date

07.12.2023

Rejection of complaint and closure of case – Tesla Norway AS

Datatilsynet refers to your complaint dated 7 May 2020 regarding the exercise of your right of access against Tesla Norway AS, and Datatilsynet's last letter to you dated 29 June 2020 with information about the status of the case.

Background

We informed you on 29 June 2020 that this is a so-called cross-border case. The case is cross border because Tesla Norway AS is an establishment of Tesla International B.V., which is established in more than one EEA country and the processing in question takes place in the context of the activities of such establishments. To ensure uniform application of the GDPR in the EEA, data protection authorities across the EEA must cooperate in the handling of cross-border cases.

The Dutch Data Protection Authority has acted as lead supervisory authority in the handling of your complaint. Datatilsynet, and all other data protection authorities in the EEA, have been involved as concerned supervisory authorities.

The lead supervisory authority has investigated the matter based on your complaint and concluded that your complaint should be rejected and that the case be closed. The lead supervisory authority has investigated the subject matter of your complaint to the extent appropriate in accordance with Article 57(1)(f) GDPR and, based on such investigation, they have not found any infringement of the GDPR. All concerned supervisory authorities, including Datatilsynet, agree with such conclusion.

Please find attached a letter from the lead supervisory authority. The letter explains how your complaint has been handled and the reason as to why your complaint was rejected.

As your complaint is to be rejected, the supervisory authority that received your complaint – in this case Datatilsynet – is the one which will adopt the final decision pursuant to Article 60(8) GDPR.

Decision

We therefore adopt the following decision in this case:

The complaint with reference number 20/02345 is rejected.

Ability to appeal

This decision has been adopted by Datatilsynet in accordance with Article 56 and Chapter VII of the GDPR, and can therefore not be appealed to the Norwegian Privacy Appeals Board pursuant to Section 22(2) of the Norwegian Personal Data Act (*in Norwegian: personopplysningsloven*). This decision can nevertheless be challenged before Norwegian courts in accordance with Article 78(1) GDPR.

Duty of Confidentiality

Parties to this matter have a duty of confidentiality under Section 13(b) of the Norwegian Public Administration Act regarding the information they receive about the complainant's identity, personal matters and other identifying information, and such information can only be used to the extent necessary to safeguard their interests in this case. Any breach of this duty of confidentiality can be punished pursuant to Section 209 of the Norwegian Penal Code.

In light of the above, we have now closed our case on this matter.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Senior Legal Adviser

This document is electronically approved and therefore does not require a handwritten signature.

Copy to: Tesla Norway AS

Attachment: Conclusion of the lead supervisory authority

TELENOR ASA
Postboks 800
1331 FORNEBU

By email to
eirik.h.andersen@telenor.com
tonje.orseth@telenor.com

Your reference

Our reference
20/03771-17

Date
26.07.2023

Decision – Google Analytics – Telenor ASA

1. Introduction

The Norwegian Data Protection Authority (“Datatilsynet”, “Norwegian SA”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“GDPR”)¹ in Norway.

We refer to our advance notification of a reprimand to Telenor ASA (“Telenor”, “you”, “your”) for having breached Article 44 GDPR, dated 28 February 2023. We also refer to the response to our advance notification, submitted by Telenor on 28 March 2023.

The present decision has been taken in accordance with the cooperation mechanism set out in Article 60 GDPR, in cooperation with the concerned supervisory authorities.

2. Decision

Pursuant to Article 58(2)(b) GDPR, we issue a reprimand to Telenor for having transferred personal data to a third country without complying with the conditions laid down in Chapter V GDPR, in violation of Article 44 GDPR.

3. Facts and background of the case

3.1 101 complaints from noyb – European Center for Digital Rights

Following the Court of Justice in the European Union (“CJEU”) ruling on 16 July 2020 in *C-311/18 – Facebook Ireland and Schrems* (“Schrems II judgment”), noyb – European Center for Digital Rights (“noyb”) lodged 101 complaints to several data protection authorities in the European Economic Area (“EEA”). All complaints concerned different European websites’ use of Google Analytics (“GA”) or Facebook Connect.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2018] L 119/1.

Based on the Schrems II judgment, noyb's complaints claim that the European websites' integration of Google Analytics and Facebook Connect causes European citizens visiting the websites to have their personal data transferred to the U.S. without a valid basis for transfer pursuant to Chapter V GDPR.

To ensure cooperation between every complaint-receiving supervisory authority ("SA") in the handling and enforcement of the 101 complaints, the European Data Protection Board ("EDPB") established a task force. This task force held regular meetings to organise and coordinate the complaints-handling process, and it has functioned as a forum for relevant discussions related to the subject matter of the complaints. It has also produced written documents, such as the questions provided to you in the order to provide information. Additionally, the task force prepared an order to provide information to Google in relation to the processing of personal data in Google Analytics.

Please note that all SAs participating in the task force have done so on a voluntary basis, and that SAs in no way are bound by the work of, or conclusions reached by, the task force.

3.2 Google Analytics

According to Google, "Google Analytics is a measurement service that allows customers to measure traffic to their properties, including website owners who wish to measure traffic to their websites. The analytics services are a popular category of service offered by multiple providers and are considered by many as an essential tool for operating a website. Website owners may use web analytics services such as Google Analytics to help them understand how their users interact with their site and services."²

3.3 Complaint against Telenor

On 17 August 2020, noyb lodged a complaint against the website www.telenor.com ("the Website") with the Austrian Data Protection Authority ("DPA"). In accordance with Article 80(1) GDPR, noyb is representing the data subject in Austria ("the complainant").

Pursuant to Article 4(23)(b), the processing of personal data subject to the complaint was assumed to be cross-border in nature. As Norway is the place of Telenor's central administration in the EEA, its main establishment within the meaning of Article 4(16)(a) GDPR is in Norway. In accordance with Article 56(1) GDPR, The Austrian DPA therefore transferred the complaint to the Norwegian SA.

On 17 August 2020, the complainant visited the Website while being logged in to the Google account associated with their email address. As a controller, Telenor had embedded the HTML code for Google Services, including Google Analytics, on the Website. The use of Google Analytics is subject to the *Google Analytics Terms of Service* and the *Google Ads Data Processing Terms*. According to the terms, Google is the contractual partner of the controller, processes personal data on behalf of the controller, and qualifies as the controller's data processor under Article 4(8) GDPR.

² Statement by Google, 9 April 2021.

In the course of the complainant's visit on the Website, Telenor processed the complainant's personal data – at least the IP address and cookie data. The complainant alleges that according to the HTTP Archive format ("HAR")³ data of the Website visit provided by them, some of this data was transferred to Google. Pursuant to point 10 of the *Google Ads Data Processing Terms*, Telenor has agreed that Google may store and process personal data

"in the USA or any other country in which Google or any of its Subprocessors maintain facilities."

The complainant maintains that such a transfer of their personal data from Telenor in the EEA to Google or its sub-processors in the USA (or any other non-EEA country) requires a legal basis under Article 44 *et seqq.* GDPR.

As the CJEU invalidated the "EU-U.S. Privacy Shield" decision in the Schrems II judgment, Telenor can no longer base the data transfer to Google in the U.S. on an adequacy decision under Article 45 GDPR. Telenor may also not base the data transfer on standard data protection clauses under Article 46(2)(c) and (d) if the third country receiving the personal data does not ensure adequate protection, under EU law, of the personal data transferred pursuant to those clauses.

In the Schrems II judgment, the CJEU explicitly found that further transfers to companies that fall under 50 U.S. Code § 1881a ("FISA 702") violate the relevant Articles in Chapter V GDPR, Article 7 and 8 and the essence of Article 47 of the Charter of Fundamental Rights of the European Union. Any further transfer of personal data would therefore violate the fundamental right to privacy, data protection and the right to an effective remedy to a fair trial.

Google qualifies as an *electronic communication service provider* within the meaning of 50 U.S. Code § 1881(b)(4). As such, they are subject to U.S. intelligence surveillance under FISA 702. As apparent by the "Snowden Slides" and Google's own Transparency Report, Google is actively providing personal data to the U.S. government under 50 U.S. Code § 1881a.

Consequently, Telenor is unable to ensure an adequate protection of the complainant's personal data that is transferred to Google. Nevertheless, as of 12 August 2020, Telenor and Google have attempted to rely on standard data protection clauses for data transfers to the U.S., as evidenced by point 10.2 of the *New Google Ads Data Processing Terms*.

Such practice ignores the Schrems II judgment, which puts Telenor under a legal obligation to refrain from transferring the complainant's personal data – or any other personal data – to Google in the U.S. More than one month after the judgment, Telenor had still not refrained from this processing.

³ HAR is a JSON-formatted archive file format for logging a web browser's interaction with a website.

In its complaint, noyb requests that the NO SA fully investigates the complaint under Article 58(1), immediately imposes a ban or suspension of any data flows from Telenor to Google in the U.S., and imposes an effective, proportionate and dissuasive fine against Telenor under Article 83(5)(c).

3.4 The Norwegian Supervisory Authority's investigation

Following noyb's complaint and the subsequent transferral of the complaint from the Austrian SA to the Norwegian SA, we sent Telenor an order to provide information on 18 December 2021. The questions in the order to provide information were prepared by the aforementioned EDPB task force. Telenor asked for an extension on the deadline to reply to the order to provide information, and as per Telenor's request, we extended the deadline from 25 January 2021 to 8 February 2021. Telenor submitted its response to the Norwegian SA on 8 February 2021.

3.4.1 Telenor's response to the order to provide information

Controllership, purpose and use of Google Analytics:

Telenor stated that the decision to embed Google Analytics on the Website was made by Telenor. As such, Telenor is the data controller. Google is a data processor in the use of Google Analytics on the Website, pursuant to the *Google Analytics Terms of Service* and *Data Processing Terms* applicable to Google Analytics.

Telenor also stated that the Website is aimed at website visitors internationally, and that therefore, data subjects from several EEA states may systematically have been subject to processing through Google Analytics on the Website.

Google Analytics was implemented before the Schrems II judgment and remained active on the Website up until 15 January 2021. On that date, Telenor completed a planned disabling of the tool as part of a revamp of the site and move to a new CMS system. At the time you responded to our order to provide information, the use of Google Analytics was decommissioned. Google Analytics was embedded on the Website to provide basic, aggregated website analytics data about the use of the site in order to optimise and improve the site layout and content. At the time Google Analytics was chosen, it was deemed a basic and easy-to-implement solution that provided the necessary analytics functionalities to cover Telenor's minimal needs.

Data localisation:

According to the information available to you, no data localisation options, including to the U.S., has been or is available when using Google Analytics. Based on information provided by Google, the data collected by Google Analytics is processed in the data center closest to the location of the user. As Google does not offer Google Analytics with region-based processing, it cannot, according to Google, be accurately determined in which country/countries Google processes such data. Google's data centers are located in several countries in North America, South America, Europe and Asia.⁴

⁴ <https://www.google.com/about/datacenters/locations/>, last visited 5 June, 2023.

Data collection:

As regards data collection using Google Analytics, you state – referencing the *Google Ads Data Protection Terms: Service Information* – that the personal data elements collected by Google Analytics are limited to online identifiers, including cookie identifiers, internet protocol (“IP”) addresses, device identifiers and client identifiers. To reduce the privacy implications of the Website’s monitoring and IP address collection, you have enabled the IP anonymisation feature of Google Analytics. It is your understanding that the identifiers listed above cannot be regarded as personal data in the context of your use of Google Analytics, as the IP anonymisation process has severed any link to an individual.

You have stated that the IP anonymisation feature of Google Analytics ensures that IP addresses from website visitors are anonymised (by removing the last octet of IPv4 addresses or removing the last 80 bits of IPv6 addresses) at the earliest possible time after data has been received by Google Analytics (i.e., the Analytics Collection Network), and before any subsequent processing takes place, including access to the data by you.

According to information you have received from Google, the IP anonymisation process takes place in the memory of the recipient webservers of Google Analytics only (i.e., data is never written to disk) and is deleted from memory rapidly. Only an extremely limited number of Google Data Center personnel have access to the relevant server memories, and such access is to your understanding never utilised for any direct processing purposes, only for technical system maintenance by Data Center personnel. Google logs all such access. Google has informed you that it would not be possible to extract such data following a potential legally binding authority request.

You assert that the only personal data collected by Google Analytics on the Website and subsequently processed by you in the context of Google Analytics has been IP addresses.

Transfers of personal data to third countries:

In late August 2020, you initiated a review project to assess agreements entered into by Telenor in light of the Schrems II judgment. You considered the Schrems II judgment to apply to your use of Google Analytics, as the agreement is entered into with Google as a U.S. data processor of Telenor.

Any transfer of personal data to Google is carried out subject to the SCC’s Module Two.

You have not carried out a thorough review of potential third country legislation, as it, according to information from Google, is not possible to determine the exact location of processing. This is due to Google applying the user’s proximity to the data center as one of the primary deciding factors for the processing location. You are aware of the CJEU’s interpretation of U.S. law, specifically FISA 702 and Executive Order 12333, and your focus has therefore been to ensure that appropriate technical and organisational measures are implemented to prevent unauthorised access to personal data. Moreover, Google has confirmed that it will not be possible for foreign authorities to gain access to the IP addresses collected prior to the anonymisation process.

You have summarised the supplementary measures implemented by you and Google as follows.

Firstly, Google has established policies and procedures for handling authority requests for user data from authorities across the world. According to Google, any request for customer data is handled by a team of qualified lawyers, and the requests are carefully reviewed to make sure they satisfy requirements in applicable laws.

Secondly, Google has, through their IP anonymisation feature, made available a technical measure preventing the full IP addresses from being processed in manner that allows access by public authorities. This process is coupled with strict controls regarding privileges for access to the production environment of the Analytics Collection Network.

In terms of supplementary measures implemented by you, you have applied a redaction script as an additional measure on the Website to prevent personal data unintentionally being shared with Google.

You are of the opinion that the SCC's, in addition to the supplementary measures adopted by Telenor and Google, would guarantee the contractual obligations as laid out in the SCCs.

Your website analytics at present:

According to your privacy policy, you now use Adobe Analytics as your web analytics vendor. Adobe Analytics processes IP addresses before deletion to allow geo-locating on municipality and city level, which allows you to filter your anonymous web visitors by municipality and city. IP addresses are not visible to you because they are automatically removed after processing.

Adobe Analytics is a Software-as-a-Service (SaaS) that leverages cloud hosting. They use Adobe-owned servers in a Data Processing Center (DPC) in London for processing and storage.⁵

3.4.2 Advance notification of a reprimand

The information provided by Telenor did not mitigate our concerns regarding the lawfulness of the use of Google Analytics. On 28 February 2023, we therefore sent you an advance notification of our *intent to issue a reprimand to Telenor for having transferred personal data to a third country without complying with the conditions laid down in Chapter V GDPR, in violation of Article 44 GDPR*.

3.4.3 Telenor's response to the advance notification

The Norwegian SA received Telenor's response to the advance notification on 28 March 2023. We will go through Telenor's arguments in more detail below, but the main legal arguments can be summarised as follows:

⁵ <https://www.telenor.com/privacy-policy/>, last visited 5 June, 2023.

- The Norwegian SA has not sufficiently distinguished the different roles of the parties, i.e., when Google is a controller and when Google is a processor.
- The Schrems II judgment related to the transfer of all or part of the personal data in clear text, which is substantially different from the processing activities in the present case.
- The Norwegian SA has not documented a clear preponderance of probability relating to the findings of transfers to the U.S. and that FISA 702 applies in practice. When issuing a reprimand stating that provisions of the GDPR have been infringed, European Convention on Human Rights (“ECHR”) Article 6 requires that there must be established a clear preponderance of probability.
- The processing of personal data in question does not constitute cross-border processing.
- For visitors within the EEA, the IP address is not transferred to the U.S., as the IP address of European visitors are pseudonymised through the IP anonymisation in the memory of Google servers located in Europe.
- Telenor had a valid legal basis for transfer. FISA 702 does not apply to Google Analytics in practice, and the transfer did not constitute an infringement of Chapter V GDPR.

3.5 Statement by Google

On behalf of the EDPB taskforce, the Austrian DPA sent a questionnaire to Google regarding Google Analytics and supplementary measures. In a letter dated 9 April 2021, Google responded to the questions. Google lists the legal, organisational and technical supplementary measures they adopted after the Schrems II judgment. According to their statement, Google has implemented a legal review of data requests, notification of customers before disclosure, and publishes a Transparency Report on data requests. Additionally, they have, *inter alia*, implemented measures in relation to encryption, data access, pseudonymity, data minimisation, and adopted strict data security and data privacy policies.⁶

4. Relevant GDPR requirements

4.1 Material and territorial scope

Article 2(1) GDPR provides that the Regulation applies to “the processing of personal data wholly or partly by automated means (...”).

What constitutes “personal data” is defined in Article 4(1) GDPR 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 (...).”

Article 4(2) GDPR defines “processing” as:

⁶ Statement by Google, 9 April 2021.

“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, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

As regards the territorial scope of the GDPR, Article 3(1) establishes that the Regulation:

“applies to the processing of personal data in the context of the activities of an establishment of a controller (...) in the Union, regardless of whether the processing takes place in the Union or not.”

4.2 Controller and processor

Pursuant to Article 4(7) GDPR, “controller” means:

“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (...).”

Pursuant to Article 4(8) GDPR, “processor” means:

“a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.”

4.3 Cross-border processing

Article 4(23) stipulates that cross-border processing means either:

- (a) *“Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member state; or*
- (b) *“Processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.”*

4.4 Transfers of personal data to third countries

Transfer of personal data from the EEA to third countries is regulated by Chapter V GDPR.

Pursuant to Article 44 GDPR, the general principle for transfers reads as follows:

“Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country (...) shall take place only if, subject to the other provisions of this Regulation, the conditions in this Chapter are complied with by the controller and processor(...). 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 GDPR further foresees different tools for transfer to ensure an equivalent level of protection for natural persons as provided for in the EEA and required by Article 44 GDPR.

Relevant tools for transfers:

Adequacy decisions, Article 45(1) GDPR:

“A transfer of personal data to a third country (...) may take place where the Commission has decided that the third country (...) in question ensures an adequate level of protection. Such transfer shall not require any specific authorisation.”

Appropriate safeguards, Article 46(1) GDPR:

“In the absence of an [adequacy decision] (...) a controller may transfer personal data to a third country (...) 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.”

Pursuant to Article 46(2)(c), the appropriate safeguard may be provided for, without requiring any specific authorisation from a supervisory authority, by

“Standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).” (“SCCs”)

Schrems II judgment:

In the Schrems II judgment, the CJEU declared the “EU-U.S. Privacy Shield” decision pursuant to Article 45(1) GDPR invalid, as American intelligence and surveillance laws undermined the level of protection for data subjects in the EEA guaranteed by the GDPR. Equally, the CJEU stated that the use of SCCs may not in themselves be sufficient to ensure that level of protection, in which case the implementation of supplementary measures may be necessary. The purpose of such supplementary measures is to ensure that personal data is not processed beyond what is necessary in a democratic society. The EDPB has issued recommendations on supplementary measures⁷ (“EDPB Recommendations”).

⁷ See Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, available on https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, last visited 5 June 2023.

5. Our assessment of the case

5.1 Main legal questions

There are three main legal questions arising from this case, namely;

- i) Whether or not personal data was processed in the context of the Google Analytics tool,
- ii) Provided that personal data was processed, whether or not this personal data was transferred to the U.S., and
- iii) Provided that the personal data was processed and transferred to the U.S., whether or not this transfer infringed Chapter V GDPR, also considering the Schrems II judgment.

In the following, we will assess these three questions in addition to other relevant elements of the case.

5.2 Scope of the Norwegian SA's investigation

Our investigation into your use of Google Analytics is limited to the time period from the CJEU's Schrems II judgment to your discontinuation of Google Analytics, i.e. between 16 July 2020 and 15 January 2021 – a time period of six months.

We have not investigated Google's potential further processing of the personal data subject to the complaint, as this was not within the scope of the complaint.

Furthermore, we have not investigated your use of the new web analytics vendor implemented on the Website.

5.3 Whether the processing in question constitutes cross-border processing

In our order to provide information dated 18 December 2020, we laid down an assumption stating that the processing of personal data within the context of Google Analytics on the Website was cross-border in nature according to Article 4(23)(b) GDPR. This assumption was based on the fact that the Telenor Website has a global reach, attracting visitors from both the EEA and the rest of the world, and that the Website's default language is English. In line with Article 4(23)(b), we assumed that the processing of personal data through Google Analytics on the Website substantially affected or was likely to substantially affect data subjects in more than one Member state. As such, we considered the processing to be cross-border in nature.

In your response to our order to provide information dated 8 February 2021, you did not contradict this assumption. Furthermore, you also stated that:

"The telenor.com site is open and accessible to any website visitor from around the globe. Telenor.com is the main corporate website of the Telenor Group, the site is

aimed at visitors from all around the globe. As such, data subjects from any European Member State may have been subject to the processing of the Tool.⁸

Following this, we concluded that the processing constituted cross-border processing within the meaning of Article 4(23)(b) in our advance notification with the following statement:

"The processing of personal data on the Website substantially affects or is likely to substantially affect data subjects in more than one Member State, as the target audience of the site are customers and stakeholders of Telenor's subsidiaries internationally. Thus, the processing constitutes cross-border processing pursuant to Article 4(23)(b) GDPR.⁹"

In your response to our advance notification, you state that we have not provided any grounds to substantiate why we have concluded that the processing through Google Analytics on the Website constitutes cross-border processing. You are of the opinion that there is no cross-border processing of personal data through Google Analytics on the Website within the meaning of Article 4(23)(b) GDPR.

You argue that there is a certain threshold for the processing to "substantially affect or is likely to substantially affect data subjects in more than one Member State, and that this threshold is not met in the present case. Furthermore, you state that the Website is aimed at corporations and companies and not at individual data subjects per se, and that it does not offer services or products to customers in Norway or any other country. You also state that your statistical overview shows that the number of individuals from other EEA countries who visit the website is low, and that, as per February 2023, the top three countries from which the Website was visited were Pakistan, Norway and India. In your view, this speaks to the fact that the processing does not substantially affect a significant number of data subjects in several Member States. Against this background, you are of the opinion that the processing does not constitute cross-border processing.

Article 4(23)(b) establishes two conditions that must be met in order for the processing to be considered cross-border; the processing must take place in the context of the activities of a single establishment of a controller or processor in the Union, and the processing must substantially affect or be likely to substantially affect data subjects in more than one Member State.

The starting point for the assessment of whether the processing is cross-border or not, is the processing operation itself. In this case, the processing in question is the alleged collection and subsequent transfer of personal data to a third country through Google Analytics, embedded on the Website by Telenor.

As this processing took place in the context of the activities of a single establishment of Telenor in the Union, the first condition of Article 4(23)(b) is satisfied.

⁸ Response from Telenor ASA to the questions posed by Datatilsynet on 18 December 2021, p. 1, question 4.

⁹ Advance notification, point 3.3.1

When it comes to the second condition, namely that the processing must substantially affect or be likely to substantially affect data subjects in more than one Member State, we agree with Telenor that not all cross-border processing activity falls within the definition of cross-border processing in Article 4(23)(b). As you state, this is also the position of the EDPB.¹⁰ We also agree that the fact that a website is accessible to anyone in the EEA with an Internet connection does not automatically mean that cross-border processing is taking place.

However, the processing in question does meet the threshold that Article 4(23)(b) sets out for the following reasons. As also stated in the above-mentioned EDPB Guidelines, Supervisory Authorities will interpret “substantially affects” on a case-by-case basis, taking into account the context of the processing, the type of data, the purpose of the processing, as well as several listed factors.¹¹

Going off the list of factors, the collection and subsequent transfer of personal data to a third country through Google Analytics on the Website can have “unlikely, unanticipated or unwanted consequences for individuals”.¹² A person visiting the website might not be aware that their personal data is being collected and subsequently transferred to the U.S., where it can be subject to U.S. intelligence surveillance. This type of processing is intrusive, uncomfortable, and is likely to substantially affect the data subjects.

Furthermore, the processing in question does not happen in plain sight and is difficult to follow for an individual. Again, some visitors might not even be aware that their personal data were being collected through Google Analytics when visiting the Website.

Moreover, the processing clearly affects data subjects in more than one Member State. The Website is the main corporate website of the Telenor Group, which has owner interests and shareholders in several countries inside and outside the EEA. Accordingly, the website is aimed at visitors from all around the globe, including the EEA, and arguably especially at visitors from countries where the Telenor Group has subsidiaries, which includes EEA countries such as Sweden and Denmark. Your statistical overview also demonstrates that Norway, Sweden, Denmark and Germany are among the top ten countries from which the Website is visited as per February 2023.¹³

Taking this into account, we have found the processing in question to substantially affect, or to be likely to substantially affect, data subjects in more than one Member State. As such, the processing constitutes cross-border processing within the meaning of Article 4(23)(b).

5.4 Competence of the Norwegian Supervisory Authority

¹⁰ Guidelines 8/2022 on identifying a controller or processor’s lead supervisory authority, Version 2.0, Adopted on 29 March 2023, para. 7.

¹¹ Ibid, para. 12.

¹² Ibid, bullet point eight.

¹³ Annex 1from Telenor: «Telenor.com | Besøk topp 50 land | Februar 2023».

As per point 5.3, the processing of personal data constitutes cross-border processing within the meaning of Article 4(23)(b).

Norway is the place of Telenor's central administration in the EEA. As such, the main establishment of Telenor, within the meaning of Article 4(16)(a) GDPR, is in Norway. The Austrian SA therefore transferred the complaint to the Norwegian SA in accordance with Article 56(1) GDPR.

Therefore, the Norwegian SA is the competent SA and acts as the lead supervisory authority in this case.

5.5 Controller and processor

5.5.1 General overview

Controller:

The complainant has identified Telenor as the controller in its complaint. In your response to us, you stated that the decision to embed Google Analytics on the Website was made by Telenor.

Therefore, we find it to be undisputed and clear that you "determine(d) the purposes and means of the processing of personal data" subject to the complaint, and therefore acted as a controller pursuant to Article 4(7) GDPR.

Processor:

The complainant further identifies Google in the U.S. as Telenor's processor in relation to the personal data processed in Google Analytics. In your response to us, you state that Google is the data processor in the use of Google Analytics on the Website, as stated in the *Google Analytics Terms of Service* and *Data processing Terms* applicable to Google Analytics. Furthermore, you have entered into SCCs with Google, using Module Two of the SCCs.

Against this background, we find it to be undisputed and clear that Google "processes(d) personal data on behalf of" you within the context of Google Analytics, and therefore acted as a processor pursuant to Article 4(8) GDPR.

Seeing as neither the complainant nor you have addressed Google Ireland Limited in relation to the processing of personal data in question, we have not investigated if, and to what extent, they are involved in the processing. Thus, we are assessing the case on the premise that a data subject in Austria visited the Website, and whether or not the complainant's personal data subsequently was unlawfully transferred from the EEA to the U.S. through your use of Google Analytics.

5.5.2 The roles of Telenor and Google

In your response to our advance notification, you claim that the Norwegian SA does not distinguish between data elements collected by Google as a data processor for Telenor in its

provision of Google Analytics, and personal data collected by Google as a data controller with respect to its provisioning of services to data subjects.¹⁴

You state that you are responsible as a controller and data exporter for the data collected through the use of Google Analytics, namely:

- IP addresses;
- Unique identifier that identifies the browser/device used to visit the Website (“cookie ID”);
- Unique identifier used to identify the Website operator (in this case the account ID of Telenor);
- Address and HTML title of the Website (i.e. Telenor.com + subdomains); and
- Information on browser, operating system, screen resolution, language settings as well as date and time of access to the Website.

Furthermore, you state that where Google acts as data controller, any transfer of personal data by Google falls outside the responsibility of Telenor. Google is the controller when it comes to the processing of personal data that happens when a visitor visits the Website while being logged into their account. Where a visitor is logged into their account in the browser, this is a processing activity that occurs in the relationship between Google as a data controller and the individual using Google services such as a Google account. These processing activities occur by virtue of a contract entered into between Google and that particular user, and falls outside the processing activities and responsibilities of Telenor.

The Norwegian SA agrees with Telenor that there likely exist situations where Google is an independent or joint controller in relation to analytics data. However, our proceedings only concern the processing carried out in Google Analytics by Google as a data processor for Telenor, i.e. the above list of data collected through your use of Google Analytics. The current case does not concern how Google processes Google account data.

Nonetheless, in assessing whether the data in scope constitutes personal data, it is necessary to assess whether the data subject is *identifiable*, and this includes looking at *all* possibilities Google may have for identification.

5.6 Whether personal data was processed in Google Analytics

In order for the GDPR to apply, “personal data” pursuant to Article 2(1) must be processed. Therefore, the complainant needs to be identified or identifiable, directly or indirectly, by the data processed in Google Analytics.

Online identifiers, such as IP addresses and information stored in cookies, can be used to identify a user, in particular when combined with similar types of information. This is illustrated by Recital 30 GDPR, whereby:

¹⁴ Telenor’s Response to Advance notification of a reprimand p. 5.

“Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers (...). This 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 order to assess whether the complainant is identifiable through the data processed in Google Analytics, thus making it personal data pursuant to Article 4(1) GDPR, it must be assessed how Google Analytics works, and whether the complainant is identifiable to Telenor or Google.

Telenor has implemented Google Analytics on the Website by inserting a JavaScript command (a tag), which was specified by Google, into the source code of the Website. While the page is loading in the browser of the visitor, the JavaScript code is now loaded from the servers of Google and executed locally in the visitor's browser. A cookie, under the domain of the website operator, is set by this JavaScript code. Among other elements, a permanent unique identifier is set in the cookie value. This unique identifier is generated and managed by Google. Telenor, however, can read the value.

On the basis of the HAR data, the following data was processed when the complainant visited the Website:

- Unique identifier(s) that identifies the browser/device used to visit the Website, as well as a unique identifier that identifies the Website operator, in other words the Google Analytics account ID of the Website operator,
- Address and HTML title of the Website,
- Information on browser, operating system, screen resolution, language settings, as well as the time and date the Website was accessed by the complainant,
- The complainant's IP address.

As regards IP addresses, it is worth noting that the anonymisation process is carried out on Google's servers. In other words, the IP address is sent to Google before it is anonymised.

The CJEU has already ruled that IP addresses in most circumstances are to be considered as personal data.¹⁵ In our view, IP addresses still qualify as personal data even though the means of identifiability lie in third entities. Additionally, IP addresses can be combined with further elements in order to make the data subject identifiable.

As these unique identifiers are set with the specific purpose to differentiate individuals, where differentiation was not possible before, they contribute to making the individual identifiable. In this regard, we note the findings of the Austrian SA in a similar case, also referring to a decision by the European Data Protection Supervisor, that these Google Analytics identifiers in principle qualify as personal data.¹⁶

¹⁵ See judgments C-597/19 and C-582/14.

¹⁶ See page 27 of the decision in question, available on <https://noyb.eu/sites/default/files/2022-04/Bescheid%20geschw%C3%A4rz.pdf>, last accessed 13 June 2023.

Even if unique identifiers per se would not make individuals identifiable, they can also be combined with further elements.

In this case and as already mentioned, the IP address and cookie identifiers were combined with, *inter alia*, the address of the specific website the complainant visited, the time and date of the website visit, as well as metadata about the browser and operating system. While the latter may appear seemingly innocuous, the combination of settings and parameters of the browser and the operating system may sometimes be sufficiently unique to lead to so-called device fingerprinting.

Therefore, both you and Google have several elements that combined can enable you to single out visitors, including the complainant, on the Website where Google Analytics was implemented. The GDPR does not require the controller or processor to know the name or physical address of the visitor – it suffices that it would be possible to identify an individual, also relying on additional data from other sources. As illustrated by Recital 26, the *singling out* of individuals may be sufficient to make them identifiable.

Additionally, the complainant was logged into their Google account at the time the Website was visited. As shown by Google's statement, the implementation of Google Analytics on a website enables Google to receive information that a specific Google account has visited that website. Even though Google states that certain settings must be enabled in order for them to process such information, it must be noted that the definition of personal data is based on whether it is technically possible to identify an individual, not whether a party chooses to do so in practice. In our understanding, tweaking the relevant settings would affect the latter aspect, but not necessarily the former.

Furthermore, the fact that you consider Google your data processor and have entered into a data processing agreement with them in the context of your use of Google Analytics, would also seem to indicate that the contracting parties are of the opinion that personal data is being processed.

Taking all of this into account, as a result, we find that the data in question is to be regarded as personal data within the meaning of Article 4(1) GDPR.

5.7 Whether a transfer of personal data to the U.S. has taken place

In your response to our advance notification of a reprimand, you state that personal data in clear text was not transferred to the U.S. for processing in Google Analytics. You had implemented the IP anonymisation feature in Google Analytics. When applying this feature, the IP address will be transmitted to the Google server closest to the Website visitor for IP anonymisation and subsequent return of the cookie ID. The IP anonymisation process occurs in the memory of the server and results in an instantaneous deletion of the IP address. Google has confirmed that it is not possible for any public authority to gain access to the IP address prior to the IP anonymisation process.

You further state that for visitors within the EEA, the IP address is not transferred to the U.S., as the IP Addresses of European visitors are pseudonymised through the IP anonymisation in the memory of Google servers located in Europe. The IP address of EEA visitors is thus not exported out of the EEA, only the cookie ID. As regards Website visitors from outside the EEA, you state that you will be a data exporter under Chapter V GDPR in situations where the IP address is transferred for IP anonymisation to another third country, i.e. when the closest server location to the visitor is in a third country.

Furthermore, you state that, as a result of the Google Analytics network being hosted within the U.S., data elements such as cookie ID, website visited, operating system, device type and screen resolution will be exported to and processed within the U.S. You are responsible under Chapter V GDPR for the export of these data elements.

We find that there is no dispute surrounding the fact that all data processed in Google Analytics eventually ends up in the U.S. – some data in clear text, and other pseudonymised. We further agree that the IP addresses of EEA visitors are most likely truncated on a European server before the cookie ID is transferred to the U.S.

However, the Website has many visitors from different third countries.¹⁷ When a visitor from a third country closer to a non-EEA data centre visited the Website, they are never connected to a European server, but are connected to a Google server in a third country instead.¹⁸ As such, the IP address of the visitor is transferred to a third country before it can be anonymised. Pursuant to Article 3(1) GDPR, the Regulation “applies to the processing of personal data in the context of the activities of an establishment of a controller (...) in the Union, regardless of whether the processing takes place in the Union or not.” This means that the GDPR applies regardless of where the data subject is located.¹⁹

In any case, as explained above, there are several data categories which in themselves or in combination constitute personal data, including the visitor’s unique identifier (cookie ID), the time of the visit and metadata about the browser and operating system. Even if IP addresses are disregarded, we find that the totality of the data transferred still constitute personal data.

Against this background, we find that personal data was transferred to the U.S. through the use of Google Analytics on the Website.

5.8 Whether the transfer of personal data infringed Article 44 et seqq. GDPR

In your response to our advance notification, you state that Telenor had a valid legal basis for transfer, that the data was not at risk for authority requests under FISA 702, that the transferred data were trivial in nature and would not have entailed an infringement of the

¹⁷ Annex 1 from Telenor: «Telenor.com | Besøk topp 50 land | Februar 2023».

¹⁸ <https://support.google.com/analytics/answer/11598602>, last visited 14 June 2023.

¹⁹ See also EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), available on https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, which on p. 10 states the following: “However, geographical location is not important for the purposes of Article 3(1) with regard to the place in which processing is carried out, or with regard to the location of the data subjects in question.”

fundamental rights of the individual if accessed by the authorities, but rather a mere interference.

As the processing activities took place within the U.S., Telenor and Google had entered into the SCCs for processors as the legal basis for transfer of personal data to the U.S. Under the SCC, Telenor acted as data exporter and Google acted as data importer. You disagree with our advance notification, where we held that the use of SCCs generally will not be sufficient for transfer of personal data to an organisation in the U.S. subject to FISA 702. You further maintain that Telenor and Google had implemented adequate supplementary measures to protect the data.

You state that although Google has been subject to access requests in general, this is not a relevant prior instance of requests for access. Furthermore, Google has confirmed publicly that during the 15-year period during which Google Analytics has been available, Google had, as of 19 January 2022, not received a single FISA request for such data. You therefore contend that FISA 702 did not apply to Google Analytics in practice.

Google LLC, as a data importer in the U.S., classifies as an electronic communications service provider within the meaning of 50 U.S. Code § 1881(b)(4). Google is therefore subject to surveillance by U.S. intelligence agencies pursuant to FISA 702, and is therefore obliged to provide the U.S. government with personal data when FISA 702 is invoked.

In Schrems II, the CJEU held that the U.S. surveillance programs based on FISA 702, E.O. 12333 and Presidential Policy Directive 28 do not meet the minimum requirements laid down in EU law in accordance with the principle of proportionality. This means that the monitoring programs based on those provisions cannot be considered to be limited to what is strictly necessary.²⁰ In other words, the CJEU found that the level of protection of personal data when transferring personal data to the U.S. is not essentially equivalent to that guaranteed in the EU.

As pointed out by Telenor, it is important to distinguish between interferences with, and infringements of, fundamental rights. Laws on governmental access which do not meet the requirements of proportionality and necessity constitute infringements by definition, and the CJEU found that U.S. surveillance laws fall within this category.

As an exception from this, we have stated in our public-facing guidance that transferring personal data *that are publicly available* to third countries without supplementary measures may possibly not constitute an infringement. This is clearly not relevant in this case, as the personal data in question are not publicly available.

Worth noting is that neither the wording of Chapter V GDPR, the Schrems II judgment, nor the practice of other EEA data protection authorities permit a so-called ‘risk-based approach’ under which data can be transferred without supplementary measures if they are not likely to be intercepted (for example if the controller believes that the data are not ‘interesting’ to third

²⁰ Schrems II judgment, para. 184.

country authorities) or if the consequences of interception are perceived by the controller as being small (for example due to the perceived nature of the data).

Furthermore, the CJEU points out that when transferring personal data on the basis of SCCs, in order to ensure that the level of protection is not undermined, it is necessary to also examine the third country's legal system with regard to access by third country authorities.²¹ Where problematic legislation on governmental access prevails, it is necessary to adopt supplementary measures in addition to the SCCs to uphold the level of protection.²²

For transfers of personal data to the U.S., it is clear that problematic legislation prevails over the SCCs, and thus supplementary measures are required unless an exception applies.

However, the EDPB has since the Schrems II judgment stated that if there is no reason to believe that the problematic legislation in question applies in practice, adopting supplementary measures is not necessary. Though this 'permittance' was formulated by the EDPB after Telenor stopped using Google Analytics, Telenor should be able to benefit from it if the conditions are met.

Concomitantly, the EDPB has specified what is required in this situation and emphasised that controllers remain accountable for their assessments:

You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below.²³

Furthermore, the EDPB has stated as follows:

You must however note that the absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor on the effectiveness of the Article 46 GDPR transfer tool that allows the transfer to proceed without supplementary measures.²⁴

It is important to note the fundamental difference between situations where there is no reason to believe that personal data are in practice covered by problematic legislation (in Norwegian: *ingen grunn til å tro at loven i praksis får anvendelse*), and situations where personal data are in fact within scope of the legislation, but there is no reason to believe that authorities will utilise the access they are granted under that legislation (in Norwegian: *ingen grunn til å tro*

²¹ Ibid., para 104.

²² Ibid., para. 133.

²³ EDPB recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, para 43.3, available on https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en,

²⁴ Ibid., para. 47.

at loven i praksis vil bli anvendt). Only the former fulfils the criteria set out in the EDPB guidelines, while Telenor's arguments appear to be tied to the latter.

To be clear, the wording of FISA 702 indicates that the personal data in this case are within scope of the problematic legislation. Telenor has failed to demonstrate and document that FISA 702 is not interpreted and/or applied in practice so as to *cover* that personal data, and Telenor has not documented that it has examined the experience of other actors operating within the same sector and/or consulted the sources of information described by the EDPB. Telenor's assertion that Google has not historically received access requests regarding Google Analytics data is in itself not sufficient.

Therefore, the question at hand is whether the SCCs were supplemented by appropriate measures to prevent U.S. intelligence services processing personal data of visitors to the Website beyond what is necessary in a democratic society.

The EDPB Recommendations explain and exemplify which supplementary measures are considered by EEA supervisory authorities to be appropriate in this regard. In general, technical measures that prevent personal data being made available to the data importer in clear text would be required here.

Though it has been argued that supplementary measures are in place, it is clear that those measures do not prevent Google from having clear text access to at least some of the personal data in question, such as the combination of the visitor's unique identifier (cookie ID), the time of the visit and metadata about the browser and operating system, again noting that the scope of personal data in this case is wider than just the IP addresses.

On this background, we find that the transfer of personal data infringed Article 44 GDPR.

5.9 Conclusion

Based on the above, we find that personal data of visitors to the Website was processed in the context of Google Analytics, that those personal data were transferred to the U.S., and that this transfer infringed Chapter V GDPR.

6. Corrective measure

The complainant requests us to impose a ban or suspension of data flows from Telenor to Google in the U.S., as well as impose an effective, proportionate and dissuasive administrative fine against you.

Seeing as your use of Google Analytics was discontinued on 15 January 2021, there is no reason to impose a ban or suspension of data flows from Telenor to Google in the U.S.

We have, however, considered whether we should exercise any other corrective powers. Taking into account all elements of the case, we find a reprimand to be an adequate and proportionate corrective measure. Pursuant to Article 58(2)(b), a reprimand is a corrective measure that SAs can issue to a controller or processor where processing operations have

infringed the GDPR. The purpose of reprimands is to indicate criticism towards the identified infringements.

In your response to our advance notification, you claim that the issuance of a reprimand requires a clear preponderance of probability, as a reprimand is to be considered as punishment under the European Convention of Human Rights (“ECHR”) Article 6. You base this on the assumption that a reprimand is a “final statement of guilt” for breaching Chapter V GDPR, similar to formal warnings²⁵ under the Norwegian Public Administration Act. You state that this threshold is not met in the present case.

As the case currently stands, also taking as a basis the additional information you provided in your response to our advance notification, we find that there is a clear preponderance of probability that personal data, including the Website visitor’s unique identifier (cookie ID), the time of the visit and metadata about the browser and operating system, was transferred to the U.S. without sufficient supplementary measures where such supplementary measures were required.

In any case, we reject that a reprimand pursuant to Article 58(2)(b) is to be considered as punishment under the ECHR Article 6.

The European Court of Human Rights (“ECtHR”) has interpreted the notion of ‘criminal charge’ for the purposes of Article 6 ECHR in several of its judgments, most notably in the Engel Case.²⁶ In that judgment, the ECtHR set out three criteria for the determination of whether a charge is ‘criminal’, namely:

1. the classification of the charge in national law;
2. the nature of the offence; and
3. the degree of severity of the penalty.²⁷

The ECtHR further elaborated on what constitutes a ‘criminal charge’ in the Öztürk Case,²⁸ where it concluded that a penalty was criminal *inter alia* because it was punitive and intended to be deterrent.²⁹

Applied to the present case, it is clear that a reprimand is not classified as a criminal law penalty under Norwegian law.

As for the degree of severity of the reprimand, it has little impact on the controller and no tangible repercussions. A reprimand cannot be considered to be a measure of any considerable severity,³⁰ and it is not of a punitive nature.

²⁵ Norwegian: “Formelle advarsler”.

²⁶ Case of Engel and Others v. the Netherlands (Application no. 5100/71; 5101/71; 5102/71; 5354/72; 5370/72)

²⁷ Ibid., para. 82.

²⁸ Case of Öztürk v. Germany (Application no. 8544/79)

²⁹ Ibid., para. 53.

³⁰ In this regard, it is worth noting Recital 148 GDPR, which states that a reprimand may be issued in case of a minor infringement.

Also worth noting is that under the GDPR, only administrative fines are intended to be dissuasive, pursuant to Article 83(1), in contrast to reprimands and the other corrective measures listed in Article 58(2).

As for Telenor's representations regarding formal warnings, we note that formal warnings are not listed in the Norwegian Public Administration Act Chapter IX among the administrative sanctions that constitute a 'criminal charge' in the sense of the ECHR.

7. Right of appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.³¹

Yours sincerely

Jørgen Skorstad
Director, law

Trine Smedbold
Legal Adviser

This letter has electronic approval and is therefore not signed

Copy: noyb – European Center for Digital Rights

³¹ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

SWIMS AS
Postboks 123
0323 OSLO

*Exempt from public disclosure:
Offl. § 24 andre led*

Your reference

Our reference
20/02315-1

Date
21.06.2023

Closure of case - Swims AS

Introduction

Datatilsynet is the Norwegian Data Protection Authority and the national supervisory authority under the European Union General Data Protection Regulation (GDPR). Our task is to supervise compliance of the GDPR and oversee that both public and commercial actors do not violate Norwegian citizens' fundamental right to data protection.

We received a complaint from a customer of Swims.com on 3 March 2020, regarding the possible loss of personal data following a cyber-attack towards the warehouse of Swims AS ("Swims").

Decision

Datatilsynet has decided to close the case.

Factual background

The complainant received a message from Swims stating that Swims experienced delays in deliveries due to a cyber-attack. The Complainant explained that she requested information from Swims regarding the cyber-attack and whether her personal data was affected. As she was worried that her personal data could be lost, she filed a complaint with Datatilsynet.

Swims provided the Complainant with an answer within a week and stated that no customer information was lost. Swims informed the Complainant that the servers of their logistical partner had been encrypted by a hacker group, however it was released a few days later. According to Swims, no data was stolen or lost in the attack.

Based on the complaint, Datatilsynet sent a request for information to Swims on 19 March 2020.

Swims has explained that they experienced a security incident with their logistical partner, due to a manual error. Moreover, Swims has stated that further training has been provided to avoid a similar incident in the future and that the customers have been informed of the incident. Furthermore, Swims explained that there has been no loss, unauthorised disclosure

of, or access to personal data of their customers. Swims' logistical partner reported the cyber-attack to the police and sent a data breach notification to the Supervisory Authority in the Netherlands.

The applicable legal framework

Article 3 GDPR prescribes that the Regulation applies to the processing of personal data of data subjects in the European Union by a controller not established in the Union, where the processing activities are related to the offering of goods or services to data subjects in the Union. As Swims AS offers a service to data subjects in the EU/EEA, your processing of personal data about Norwegian citizens falls within the territorial scope of the GDPR.

We consider that this case is cross-border pursuant to Article 4(23)(a) GDPR and that we are the lead supervisory authority pursuant to Article 56(1) GDPR.

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, cf. Article 5(1)(f) GDPR. The controller shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk for the rights and freedoms of natural persons, cf. Article 32(1) GDPR.

Please note that pursuant to Article 33 GDPR, it is the controller that should carry out notification of a data breach to the supervisory authority. The processor may be authorised by the controller to notify on their behalf. In any case, the notification should be sent to the controller's lead supervisory authority.

Datatilsynet's assessment

Datatilsynet considers that there is no need for further investigation into this case and that Swims has handled the security incident in an appropriate manner. In conclusion, Datatilsynet hereby closes the case.

Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.¹

Kind regards

Tobias Judin
Head of Section

Anne Eidsaa Hamre
Legal adviser

¹ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

This letter has electronic approval and is therefore not signed

Copy: the Complainant

BRANDSDAL GROUP AS
Postboks 8104
4675 KRISTIANSAND S

Exempt from public disclosure:

Offl. § 13, jf. personopplysningsloven § 24 første ledd 2.

punktum

Your reference

Our reference
20/02313-9

Date
14.02.2024

Closure of case – Brandsdal Group AS

I. Introduction

On 5 March 2020, the Finnish Data Protection Authority (“Tietosuojavaltuutetun Toimisto”, “Finnish SA”) transferred a complaint to the Norwegian Data Protection Authority (“Datatilsynet”, “we”, “our”). The complaint was lodged by [REDACTED] (“the complainant”) against Brandsdal Group AS (“Brandsdal Group”). Brandsdal Group is a Norwegian e-commerce company that operates the website www.cocopanda.fi (“Cocopanda”).

II. Factual background – the complaint

The complainant stated that Cocopanda cancelled her order due to suspicion of fraud. In order for the complainant to regain access to her account, Cocopanda asked her to verify her identity by sending a picture of her ID card via unencrypted email. The complainant did not consider this a secure way to verify her identity. Furthermore, the complainant requested Cocopanda to erase her personal data pursuant to Article 17 GDPR. The complainant claims that Cocopanda did not comply with her erasure request.

III. Inquiry by the Norwegian Data Protection Authority

On 18 May 2020, the Norwegian Data Protection Authority sent an order to provide information to Brandsdal Group, inquiring about the issues brought up in the complaint. In their response, Brandsdal Group stated that they do not require customers to verify their identity by sending a picture of their ID cards via unencrypted email – there are alternate ways to upload this verification if the customer views email as an unsecure channel of communication. Furthermore, Brandsdal Group stated that they did not reject the complainant’s request for erasure. This fact was also communicated to the Finnish SA.

IV. Closure of case

On 18 December 2023, we asked the Finnish SA to forward a letter to the complainant. The letter informed the complainant about the delay in our processing of the complaint due to a lack of resources. On 21 December 2023, the Finnish SA informed us that they had forwarded the letter to the complainant and received a response. The complainant stated that she has settled the case with Cocopanda.

Taking into account that the complainant has settled the case with the controller, effectively mooting the issues raised in the complaint, and that the complainant did not express any wish to pursue the matter further, we consider that the matter has been resolved to the complainant's satisfaction and will close the case.

In light of the above, we consider that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR, and that the matter may be deemed to be resolved to the complainant's satisfaction. We have therefore decided to close the present case in accordance with Article 60(7) GDPR.

Kind regards

Tobias Judin
Head of Section

Trine Smedbold
Senior Legal Adviser

This letter has electronic approval and is therefore not signed

c/o Data Protection Officer
NORWEGIAN AIR SHUTTLE ASA
Postboks 115
1330 FORNEBU

*Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven § 24 første ledd 2.
punktum*

Your reference

Our reference

21/00684-8

Date

15.01.2024

Closure of case due to withdrawal of complaint

1. Background

The Norwegian Data Protection Authority (the “**Norwegian DPA**”) is the independent supervisory authority competent for performing the tasks and exercising the powers conferred on it by the GDPR¹ on the territory of Norway.

On 13 October 2020, [REDACTED] (the “**Data Subject**”) lodged a complaint pursuant to Article 77 GDPR with the Danish Data Protection Authority (the “**Danish DPA**”) concerning Norwegian Air Shuttle ASA (“**NAS**”).

The Norwegian DPA was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

2. The complaint

The details of the complaint were as follows:

- The Data Subject requested access to his personal data on 12 August 2020.
- NAS responded to the Data Subject’s message on 24 August 2020, but did not respond to the Data Subject’s access request.
- The Data Subject again requested access to his personal data on 31 August 2020, but did not receive a response.
- As the Data Subject did not get access to his personal data, he lodged a complaint with the Danish DPA.

3. Summary of how the case has been handled

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

The Danish DPA forwarded the complaint to the Norwegian DPA on 27 January 2021. On 20 September 2021, the Norwegian DPA ordered NAS to provide information regarding their handling of the Data Subject's complaint. NAS responded on 4 November 2021 and stated that the Data Subject's access request had not been handled correctly due to human error under hectic conditions during the pandemic. NAS further stated that they have now handled the Data Subject's access request.

On 18 September 2023 the Danish DPA informed the Norwegian DPA that the Data Subject is withdrawing his complaint as it is no longer relevant.

4. Conclusion

As the complaint on which this case is based has been withdrawn, the Norwegian DPA has closed its case on this matter.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Senior Legal Adviser

This letter has electronic approval and is therefore not signed

COPY TO: [REDACTED]



Norsk Hydro ASA
Postboks 980 Skøyen
0240 OSLO

Your reference

Our reference
20/01770-4

Date
12.05.2021

Closure of case - Norsk Hydro ASA

We refer to your data breach notification, received on 21 March 2019, pertaining to a data breach which was discovered on 18 March 2019. We also refer to the additional information you provided on 26 March 2019 and 21 June 2019.

Based on the information available to us, the case can be summarised as follows:

- The data breach was caused by a targeted, sophisticated and malicious attack.
- The attack culminated with the introduction of ransomware to your systems. As a consequence, the availability of personal data was adversely and severely impacted. The forensic investigations confirm that the attacker's motivation was to hamper your operations to get ransom for encrypted files.
- In order to perform the attack, the attacker accessed user names and passwords of the Active Directory. Forensic investigations carried out by yourselves as well as the Norwegian National Security Agency does not indicate that the confidentiality of personal data was affected beyond this.
- When investigations were ongoing and the extent of the data breach was still unclear, you communicated information regarding the data breach to employees and external stakeholders through various channels.
- You have since the attack implemented measures in cooperation with the Norwegian National Security Agency and other external experts in order to ensure the resilience of your systems against similar attacks in the future, hereunder:
 - Measures to manage access and reduce the risk of lateral movement and escalation of privileges
 - Measures to detect and respond to unauthorized access
 - Overall strengthening cyber securities capabilities throughout the organization, illustrated by setting cyber security as a key achievement of 2020, requiring

mandatory training of IT users, establishment and training of a cyber-crisis team, setting cyber risk management as part of your enterprise risk management process, etc.

Taking into account the above, the Norwegian Data Protection Authority does not see a need to pursue this matter further. We therefore close the case.

Kind regards

Eirik Gulbrandsen
Senior Engineer

Jade Bui
juridisk rådgiver

This letter has electronic approval and is therefore not signed

Hotel Online AS
c/o Oslo
International Hub
Oscars gate 27
0352 OSLO

Exempt from public disclosure:
Offl. § 20 første ledd B

IMI Case Rep. reference
293985

Our reference
20/02292-8

Date
03.05.2021

Closure of case

We refer to our latest request for information dated 4 January 2021 and your letter dated 23 January 2021.

A complaint has been lodged with the Norwegian SA against you, Hotel Online AS (formerly Global Travel Technology AS/European Travel Group AS). We are the leading supervisory authority as Cityhotels.no/com is a hotel portal owned by you as a Norwegian registered company with your main establishment in Norway.

The subject matter of the complaint is an alleged breach of security of processing. The complainant booked a hotel through cityhotels.no. Upon completion of the transaction, an order confirmation was given in the form of a web-page. The complainant discovered that basic manipulation of the URL of the web-page revealed order confirmations of other customers. Order confirmations include information such as the name and home address of the data subject, the hotel booked, dates of stay and price.

You acknowledge the lack of security of processing when processing personal data through your booking website www.cityhotels.no. After we made you aware of the security issue connected to the booking website, you have closed down www.cityhotels.no. You are also in the process of establishing a new booking system on cityhotels.com, with a brand new solution that you have stated will satisfy the requirements of the GDPR.

We refer to your full response to our order to provide information regarding all measures you have taken.

Generally, this type of lack of security of processing could have adverse personal data consequences. However, in the view of the Norwegian SA, you has taken adequate and appropriate measures to address the issue by closing down the website and getting data protection expertise when setting up a new booking website. In addition, we have no information that personal data of costumers has been abused by manipulating the URL.

Taking into account the above, the Norwegian SA not see a need to pursue this matter further. We therefore close the case.

Kind regards

Tobias Judin
Head of Section

Tanja Czelusniak
Legal advisor

This letter has electronic approval and is therefore not signed

Copy: Complainant

Elkjøp Nordic AS
Postboks 4303 Nydalen,
NO-0402 OSLO

***Exempt from public
disclosure:***

Offl. § 20 første ledd B

IMI Case Rep. reference
304618

Our reference
20/02353-17

Date
17.06.2021

Closure of case

We refer to our latest order to provide information dated 9 February 2021 and your letter dated 30 March 2021 concerning the data protection complaint that has been raised with the Norwegian Data Protection Authority (DPA).

We are the leading supervisory authority as Elkjøp Norway AS is a Norwegian registered organization with your main establishment in Norway.

The complaint relates to how Elkjøp Norge AS (hereinafter "Elkjøp") has processed [REDACTED] (hereinafter "complainant") personal data. The complainant believes that there has been a breach of the Norwegian Personal Data Act, including the General Data Protection Regulation (GDPR), as you have sent personal data to the wrong e-mail address, by mixing up two customer accounts. Elkjøp is said to have sent the complainant's receipt, information and payment information to another customer, without the complainant's consent.

The e-mail address of the complainant and the person who has received the complainant's emails are identical before the alpha curl, but the two accounts use different e-mail services ("Hotmail" and "Gmail" respectively). The information was supposed to be sent to [REDACTED], but has been sent to [REDACTED].

According to the complainant, there is probably a fault in your systems for costumer registration. The complainant has repeatedly contacted you to correct the error, the first time on 22 April 2020.

On 9 February 2021 the Norwegian DPA sent an order to provide information to your organization (see attachment 1).

Your organization's response

In your reply, you advise that it is your organization's understanding that the complainant accidentally entered the wrong e-mail address when he was making a purchase on your online store. As a result, the wrong costumer began to receive e-mails on the complainant's orders.

The complainant contacted you on several occasions to raise concerns about this situation and to ask for his e-mail address to be corrected. You state that unfortunately, in this case, you've had poor follow-up whereby it took a while for the correction of the customer's information, i.e. to create a new customer "card" with the correct e-mail address. The complainant's e-mail address was corrected on 27 November 2020.

You inform us that you are currently working on a new solution to more easily correct this type of errors, which will be launched in April. We refer to attachment 2 for your response in full.

Our view

The Norwegian DPA have considered the information available to us in relation to this complaint and we are of the view that the fault for registering the wrong e-mail address lies with the complainant. We therefore conclude, based on a *prima facie* assessment of the information you have provided us, that you have adequate procedures and measures in place to ensure that personal data is correctly registered.

You acknowledge that you have had poor follow-up of the complainant's request of correction of his personal data. Given that it took more than 6 months to correct the e-mail address, the Norwegian DPA is not minded to believe you have met the requirement to handle requests pursuant to Article 15-22 in the GDPR "without undue delay and no later than within one month", cf. Article 12 (3). The Norwegian DPA recognizes that Elkjøp's standard operating policies and procedures in relation to handling costumer GDPR-requests do not seem to have initially been followed in this case.

We also note that you have provided us with the information that you are currently working on a new solution to more easily correct wrongly registered personal data, and that you have a new updated training created for employees with the topic GDPR and handling of customer data.

In light of this, we do not currently intend to take any regulatory action on this complaint. However, you should know that we keep a record of all the complaints raised with us about the way organizations process personal information. The information we gather from complaints may form the basis for action in the future where appropriate.

Next steps

Our website contains significant advice and guidance about the processing of personal data and an organization's obligations under data protection law, which may help to inform any decisions you make about the processing of personal data in the future.

Should you wish to discuss this case any further, or require any clarification, please do not

hesitate to contact us.

Kind regards

Tobias Judin
Head of Section

Tanja Czelusniak
Legal advisor

This letter has electronic approval and is therefore not signed

Attachments:

- (1) Norwegian DPA's order to provide information
- (2) Elkjøp's reply to the order to provide information

In copy:

- The complainant

KOMPLETT BANK ASA
Postboks 448
1327 LYSAKER

Your reference

Our reference

20/02319-8

Date

11.11.2021

FINAL DECISION – COMPLIANCE ORDER AND REPRIMAND

We refer to our advance notification of 16 December 2020 and previous correspondence. We also refer to the answer to the advance notification from Komplett Bank ASA (Komplett Bank) of 22 January 2021 and to the e-mail with additional comments from the complainant of 10 January 2021.

1. Compliance Order and Reprimand

The Norwegian Data Protection Authority issues the following decision to Komplett Bank:

1. Komplett Bank ASA must implement measures to ensure that requests from data subjects that constitute objections against direct marketing pursuant to Article 21(3) GDPR, leads to the personal data in question no longer being processed for such purposes.
2. Komplett Bank ASA must implement measures to ensure that requests from data subjects under Articles 15–22 GDPR are answered within the time limits set forth in Article 12(3) GDPR.
3. Collectively, for having processed personal data in breach of Articles Art. 6(1), 12(1) and (3), 13(1) and (2), 21(3) and (4) GDPR, Komplett Bank ASA is given a reprimand.

We are competent to issue corrective measures pursuant to Article 58(2) GDPR.

2. Case Background

The complainant states that he has been a customer of Komplett Bank since 2016. He argues that his personal data has been processed unlawfully, as he has received direct marketing by

e-mail without having the possibility to opt out from this upon registration of his e-mail address.

The complainant further states that he, after having received the first e-mail containing direct marketing in September 2018, contacted Komplett Bank to object to this use of his personal data. Still, he again received an e-mail containing direct marketing in November 2019.

The complainant has been in contact with the Data Protection Officer of Komplett Bank on several occasions, and has documented that, on some of the occasions, more than one month elapsed before his requests was answered.

Based on information available online and provided in the initial e-mail correspondence with the Data Protection Officer, the complainant was of the understanding that the legal basis for Komplett Bank's processing his personal data was consent. When the complainant expressed this understanding in an e-mail, the Data Protection Officer wrote in response that the legal basis was not consent, but rather necessity for the performance of a contract pursuant to Article 6(1)(b) GDPR. Later, in an e-mail from the Data Protection Officer of 26 June 2020, the legal basis for processing was reported to be Article 6(1)(f) GDPR for the purpose of marketing the bank's products within the same product category towards customers, and Article 6(1)(b) GDPR for the purpose of marketing in relation to the customer benefit program for Komplett Bank Mastercard.

From the documentation we have received from the complainant, there does not seem to be a designated opt out possibility for marketing from Komplett Bank. Conversely, under the tab called 'My Consents', there is a possibility to 'approve' digital marketing via e-mail and SMS.

In a letter of 18 June 2020, Komplett Bank answered questions from the Norwegian Data Protection Authority regarding the case. Also in this letter, the legal basis for processing of personal data relevant for the case is stated to be Articles 6(1)(f) and (b) for the two above-mentioned purposes. Routines for handling access requests and the balancing of interests assessment pursuant to Article 6(1)(f) was attached.

In the letter, you write that customers who wish to opt out from direct marketing can do so by changing their consents when logged into the bank's online banking service, or by contacting customer service.

The routines for handling requests for access to personal data, attached in the letter from Komplett Bank, state that a weekly meeting is held to go through access requests. Access requests are said to be answered within one month. Further, it is stated that in some cases the time limit can be extended. Which cases that qualify for extension is not specified.

In an e-mail with additional comments from the complainant of 10 January 2021, he raises questions on compliance with Article 15(3) of the Marketing Practices Act:

‘Article 15(3) of the Marketing Practices Act and Article 15(2) ePrivacy both sets a condition that the customer must be given a possibility to object against such marketing when the electronic address is gathered. In other words, it will not be sufficient to give access to object at a later stage, e.g., on a “My Page”, as this does not fulfil the condition of simultaneousness.’

These are questions for which the Consumer Agency is competent authority (see Section 3.1 below).

In Komplett Bank’s answer to the advance notification of 22 January 2021, you have given your comments to the assessment by the Norwegian Data Protection Authority. We have implemented the comments in our assessment (see Section 4 below).

3. Legal Background

Personal data shall be processed in a lawful, fair and in a transparent manner pursuant to Article 5(1)(a) GDPR, cf. Article 1 of the Personal Data Act.

Pursuant to Article 5(2) GDPR, the controller has an independent responsibility to be in, and must be able to demonstrate, compliance with the principles relating to processing of personal data in Article 5(1) (the accountability principle).

3.1. Lawful processing of personal data

The Norwegian Data Protection Authority is not the competent authority for issues specifically regulated by the Marketing Practices Act. Pursuant to Article 15(3) of the Marketing Practices Act, consent is required in some situations. However, consent is not required for direct marketing via e-mail in existing customer relationships, on certain conditions. The Consumer Agency is competent authority for the control of companies’ compliance with the provision. Nonetheless, companies must still ensure that the processing of personal data is also in compliance with the GDPR.

To be lawful, the processing of personal data must have a basis in one of the alternatives in Article 6(1)(a)–(f) GDPR.

If a contract with the data subject is to be used as basis for the processing of personal data, the processing must be necessary for the performance of the contract to be lawful, cf. Article 6(1)(b) GDPR. The European Data Protection Board (EDPB) has stated that the processing must be *objectively necessary*. This means that the controller should be able to demonstrate how the main subject-matter of the specific contract with the data subject cannot be performed if the specific processing of the personal data in question does not occur.¹ The fact that a processing of personal data is written in the contractual terms, is neither sufficient, nor necessary for Article 6(1)(b) GDPR to be applicable.

¹ EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, para. 30.

Pursuant to Article 6(1)(f) GDPR a processing of personal data can be done lawfully if based on a balancing of interests. The processing must be necessary for the purposes of the legitimate interests pursued by the controller, which can be pursued if the interests or fundamental rights and freedoms of the data subject override these interests. This basis for the processing is divided into three. The controller must have a legitimate interest, the processing must be necessary to be able to achieve the legitimate purpose, and a balancing of this interest against, i.e., the data subjects' right to privacy must be done in the specific case.

3.2. Retroactive change of legal basis for the processing

A controller that has used one basis for their processing of personal data, cannot at a later stage go back and base an already executed processing on a different basis. If the basis that the processing originally was based on turns out to be invalid, the processing that has taken place will be unlawful. The reasoning behind this is that the controller must make the assessment at the outset of processing, and that the data subject should be able to trust that the information given about the basis for processing is correct.²

3.3. The data subject's right to object

The data subject shall at any time have the right to object to processing of personal data concerning him or her that is based on Article 6(1)(f) GDPR. The same applies to personal data processed for the direct marketing purposes, regardless of what the basis for processing is, cf. Article 21(2) GDPR. When the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes, cf. Article 21(3) GDPR.

3.4. The data subject's right to information

3.4.1. Right to information about the legal basis for processing, purpose of the processing and the right to object

A person that has their personal data processed, has the right to information about several circumstances. The information shall be given in a concise, transparent, intelligible and easily accessible form, using clear and plain language, cf. Article 5(1)(a) and Article 12(1) GDPR. This can for instance be done through a privacy statement.

When personal data is collected from the data subject, the controller shall inform, *inter alia*, of the purposes of the processing for which the personal data are intended as well as the legal basis for the processing, cf. Article 13(1)(c) GDPR. If the processing is based on point (f) of Article 6(1), the data subject shall also be informed of the legitimate interests pursued. This information shall be given at the time when the personal data are obtained.

² *EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*, para. 17.

The controller should seek to avoid confusion regarding which legal basis they apply for processing of personal data. The data subject can, e.g., get the impression that they are consenting to a specific processing, while the processing in reality is based on contract pursuant to Article 6(1)(b) GDPR.³

At the latest at the time of the first communication with the data subject, he or she shall be explicitly informed of the right to object in Article 21(1) and (2) GDPR. The information shall be presented clearly and separately from any other information, cf. Article 21(4) GDPR.

3.4.2. Time limits for answering data subject requests

If the data subject asks for the fulfilment of a right pursuant to Article 15–22 GDPR, the controller shall give an answer without undue delay and in any event within one month of receipt of the request, cf. Article 12(3) GDPR. The answer shall contain information on action taken on the request. Where necessary, taking into account the complexity and number of the requests, the time limit can be extended by two further months. If so, the data subject shall be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

4. The Norwegian Data Protection Authority's assessment

4.1. Lawful processing of personal data

Komplett Bank writes in the letter of 18 June 2020 that direct marketing towards customers is a processing of personal data that is based on a balancing of interests pursuant to Article 6(1)(f) GDPR.

Komplett Bank has attached the evaluation on balancing of interests that is made regarding the processing of personal data for the purposes of direct marketing towards customers of the bank's products within the same product category. The Norwegian Data Protection Authority is of the perception that the balancing of interests provides basis for lawful processing of personal data for this purpose pursuant to Article 6(1)(f) GDPR.

Further, you write that the processing of personal data in connection to the customer benefit program for Komplett Bank Mastercard is based on contract pursuant to Article 6(1)(b) GDPR. You write that you see it as a contractual obligation to inform participants in the benefit program about campaigns and other related benefits. The membership terms for the customer benefit program, dated 18 September 2015, point 1.1, state that Komplett Bank undertakes to inform the customers periodically about earning possibilities and possibilities to withdraw bonus points.

As mentioned, one can only use Article 6(1)(b) as legal basis for processing if the main subject-matter of the specific contract with the data subject cannot be performed if the

³ *EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*, para. 20.

specific processing of the personal data in question does not occur. To identify the main subject-matter, one should look at the nature of the service provided, the contract's purpose and essential elements. Especially, one should consider how the service is promoted or advertised to the data subject, since this can shed light on what were the mutual perspectives and expectations of the parties, as well as which reasonable expectations the customers can have regarding how their personal data will be processed.⁴

This case primarily regards a credit card service. Taken into account how Komplett Bank advertises the credit card on their own website, it seems like the essential elements that can be expected by the customer are a charge-free and non-contact credit card with until 50 days of interest-free credit, bonus point acquirement and insurances.⁵ Therefore, we assume this the main subject-matter of the service.

In other words, it does not seem like sending out offers from Komplett Bank and from the bank's collaborating partners is part of the main subject-matter of the service, even if this is written in the membership terms for Komplett Bank's customer benefit program, point 1.1.

In Komplett Bank's answer to the advance notification of 22 January 2021, you write:

'As the Norwegian Data Protection Authority points out, the main subject-matter of the customer benefit program is credit, earning of bonus points and insurance. When we send newsletters and campaigns to customers to motivate use of the credit card and promote the benefits of the benefit program, it will necessarily also include our collaborator's services, that is, insurance partners or stores where bonus points can be earned. This is all the same marketing of Komplett Bank's *own* service, that is, our service in giving out bonus points and negotiating for good terms with our collaborators.'

We agree with Komplett Bank's remark in that marketing of collaborators' services is all the same marketing of Komplett Bank's own service in this context. However, we cannot see that marketing of the service is the main subject-matter of the contract. Use of the credit card, with its benefits, bonus point acquirement and insurances, can be executed without the processing personal data for direct marketing purposes. It is therefore the Norwegian Data Protection Authority's assessment that the processing of personal data for marketing purposes on Komplett Bank's or other parties' behalf is not objectively necessary for the performance of a contract to which the data subject is a party.

Further, in Komplett Bank's answer to the advance notification of 22 January 2021, you write:

'As an illustration that it can be relevant to use alternative (b) instead of alternative (f), we can point to former legal sources. In the *travaux préparatoires* of the former Personal Data Act Article 26 (the right to opt out from direct marketing) it was expressed that it can be 'hard and unnatural to separate objective information

⁴ *EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*, para. 33.

⁵ <https://www.komplettbank.no/kredittkort/>.

connected to the contractual relationship and marketing of closely related products.⁶ Further, Article 7-7 of the former Norwegian Regulation on Data Protection made an exception for the duty to give notice for processing of customer data as part of administration and execution of the contractual obligations. This shows that it is not unnatural, considering the legal sources, to deem processing of personal data relating to marketing in existing customer relationships as ‘necessary for the performance of a contract’ and therefore with legal basis in Article 6(1)(b) GDPR’.

It is the responsibility of the controller to follow applicable data protection rules. The new Personal Data Act and the GDPR has been applicable in Norway since 20 July 2018. In the EU, the GDPR has been applicable since 25 May 2018. Article 26 of the former Personal Data Act was set aside in 2009.⁶ This case regards processing executed in the period after these dates. Former legal sources may carry limited weight in this regard.

The processing of personal data for marketing purposes on Komplett Bank’s or other parties’ behalf was not necessary for the performance of the contract. Therefore, Article 6(1)(b) GDPR cannot provide legal basis for the processing.

The processing in question was executed without a legal basis in Article 6(1) GDPR. This constitutes a breach of Article 6(1) GDPR.

In Komplett Bank’s answer to the advance notification of 22 January 2021, you have also written that you assume that our compliance order only regards the processing that relates to the case and not the activities of the bank in general. This is a correct interpretation. We have constricted the wording in the compliance order for clarification. The requirement of having a valid legal basis, however, applies generally to all processing of personal data executed by a controller.

4.2. Retroactive change of legal basis for the processing

It is not possible to retroactively “change” to another legal basis after having commenced with the processing, e.g., because the original legal basis did not cover the processing after all.⁷ Any change in the legal basis for processing shall in any event be informed to the data subjects pursuant to the duty to inform in Articles 12–14 GDPR.

The Norwegian Data Protection Authority is of the understanding that the same legal basis had been used for the processing activities in question from start to end, and that there is no kind of retroactive “change” of legal basis, e.g., from consent to contract. The fact that the complainant may have been of the understanding that this is the case, may on the other hand suggest that Komplett Bank has provided insufficient information (see Section 4.4 below).

⁶ By the Marketing Practices Act.

⁷ See *EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0*, para. 34 and *EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1*, para. 123.

Komplett Bank writes, in your answer to the advance notification of 22 January 2021, that you are willing to change the legal basis for processing of personal data for marketing of the customer benefit program:

'The Norwegian Data Protection Authority recognises that Komplett Bank has legal basis in Article 6(1)(f) GDPR for the processing of personal data concerning the marketing towards customers of the bank's own products within the same product category. Conversely, the Norwegian Data Protection Authority finds that Komplett Bank does not have legal basis in Article 6(1)(b) for processing of personal data in relation to the marketing of the customer benefit program. The Norwegian Data Protection Authority's conclusion is that this in the future will have to be based on another legal basis, for instance a legitimate interest, if the requirements are fulfilled.

We take note of this. In the future, we will base our marketing of the customer benefit program on Article 6(1)(f) GDPR.'

Further, you write:

'For the sake of good order, we would like to bring attention to the fact that we have intended no substantial difference between basing one type of marketing on Article 6(1)(f) GDPR, and the other on Article 6(1)(b) GDPR. For both processing activities, we have found the requirements in the Article 15(3) of the Marketing Practices Act to be fulfilled – meaning there is an existing customer relationship, and the marketing relates to our own services corresponding to the one that the customer relationship is built on. Whether alternative (b) or (f) is used as legal basis will then not make a difference to the processing of personal data.

[...]

Distinguishing between alternative (b) or (f) for direct marketing in existing customer relationships is still mostly of theoretical interest. It does not affect the extent or the way in which we send newsletters or marketing, and it does not affect the customers' privacy rights, including the right to reserve oneself against marketing. When we now will follow the decision of the Norwegian Data Protection Authority, and clarify that our legal basis is Article 6(1)(f) GDPR, cf. Article 15(3) of the Marketing Practices Act, this implies no difference in practice. Our potential reference to a wrong legal basis therefore has not had any negative effects for the data subjects.'

We recognise that you have considered the marketing activity in question to be in line with the requirements in Article 15(3). As mentioned, we do not have competence to examine the statement. These requirements come in addition to your duties pursuant to data protection rules. In other words, compliance with the Marketing Practices Act does not remedy breaches to the Personal Data Act.

We also recognise that if Komplett Bank had used a different legal basis for the processing from the outset, it may not have had any impact on how the processing was executed. This

does not, however, necessarily mean that the reference to an inapplicable legal basis has not had negative effects for the data subjects. Furthermore, it does not make the already executed processing lawful pursuant to data protection rules.

All processing of personal data must follow the principles of ‘lawfulness, fairness and transparency’ pursuant to Article 5(1)(a) GDPR. The principle of transparency entails that the legal basis for the processing should be transparent to the data subject from the outset. A retroactive change from one legal basis to another after the processing has started, leads to a lack of predictability for the data subjects. The controller is required to disclose the legal basis upon collection of the personal data, and must therefore have correctly identified in advance of collection what the applicable lawful basis is.⁸

The processing in question can therefore in the future be based on Article 6(1)(f) GDPR, provided that the requirements set out in that provision are fulfilled. There is, however, no room for a retroactive change to this legal basis for processing of personal data that was initially based on Article 6(1)(b).

The change of legal basis cannot remedy the inapplicability of the specified legal basis for the processing already executed.

4.3. The data subject’s right to object

The complainant has provided documentation that he, in an e-mail to the Data Protection Officer of Komplett Bank of 27 September 2018, asked you to stop sending him direct marketing. The wording he used connected to direct marketing via e-mail was: ‘Further, I ask for a guarantee that this will not repeat itself.’

The Norwegian Data Protection Authority considers this an objection pursuant to Article 21 GDPR. Upon an objection to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes, cf. Article 21(3) GDPR. The complainant still received new direct marketing from Komplett Bank after the request.

The continued processing of personal data for direct marketing purposes after the complainant’s objection to the Data Protection Officer of Komplett Bank, constitutes a breach of Article 21(3) GDPR.

4.4. The data subject’s right to information

Documentation provided by the complainant shows that there evidently is no designated opt out possibility for marketing from Komplett Bank in the online banking service. On the contrary, under the tab called ‘My Consents’, there is a possibility to ‘approve’ digital marketing via e-mail and SMS. According to the complainant, this box was pre-ticked with the answer ‘yes’ to marketing via e-mail. If this is the alternative you have referred to as a simple possibility to opt out from direct marketing from Komplett Bank, it does not provide

⁸ *EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1*, para. 123.

information in a transparent and easily accessible form. Firstly, the information indicates that the legal basis for the processing is consent. Secondly, the information can be understood in a way in which there is only a possibility to limit direct marketing from Komplett Bank that is sent electronically.

In the membership terms for the customer benefit program, dated 18 September 2015, the processing of personal data is also connected with the notion of ‘consent’, see point 4. The Norwegian Data Protection Authority assumes that these membership terms were applicable at the time of the events of the present case, and that the Personal Data Act of 2018 therefore is applicable.

A request for consent that is implemented into a longer text with different contractual terms is not a valid consent pursuant to Article 6(1)(a) GDPR.⁹ Komplett Bank does not in reality seem to have been of this conviction either. Conversely, Komplett Bank has informed us that the legal basis for this processing has been evaluated under Article 6(1)(b). Nonetheless, the membership terms gives misleading information, as it indicates that the legal basis for the processing is consent pursuant to Article 6(1)(a) GDPR. Komplett Bank has not given the data subjects information about using Article 6(1)(b) GDPR as legal basis for processing of personal data.

Assessing the information provided in combination, can lead to the person having their personal data processed believing that the legal basis is consent.

The documentation provided by the complainant on correspondence with the Data Protection Officer of Komplett Bank, also shows that he is given insufficient information about which legal basis is used for which processing activity, even if this was corrected at a later stage.

The Norwegian Data Protection Authority further cannot see that Komplett Bank made the complainant aware of his right to object to the processing of his personal data for direct marketing purposes, pursuant to Article 21(4) GDPR.

On this background, the Norwegian Data Protection Authority finds that there is a breach of Articles 13(1), 12(1) and 21(4) GDPR.

In the answer to the advance notification of 22 January 2021, Komplett Bank states that you have implemented measures to correct the wording in your communication, by clarifying that the legal basis is Article 6(1)(f). You also state that measures have been implemented to make sure that the data subjects are made explicitly aware that they have the right to object at the latest at the time of the first communication.

⁹ See especially Article 7(2) GDPR and *EDPB Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1*, para. 71.

4.4.1. Time limits for answering data subject requests

We cannot see that Komplett Bank has given the complainant information on actions taken due to his requests without undue delay, and in any event within one month of receipt of the request. We also cannot see that Komplett Bank has given the complainant information about the delay, and the reasons for the delay within one month. Several times, the complainant has experienced that more than one month has passed without receiving neither a final, nor a temporary answer to his requests. Furthermore, we cannot see that Komplett Bank's routines for handling access requests from data subjects state that the time limits in Article 12(3) GDPR are to be followed.

In the answer to the advance notification of 22 January 2021, Komplett Bank explains that the time limits was exceeded in this case due to a lack of capacity and a backlog at the customer service. In the first instance, the delay was only a couple of days after the one-month limit. Thereafter, you explain that some time was spent investigating the complainant's additional questions and comments to your answers.

Article 12(3) states that where necessary, taking into account the complexity and number of the requests, the time limit can be extended by two further months. In any case, the data subject shall be informed of the extension within one month of receipt of the request, together with the reasons for the delay. This requirement needs to be incorporating into your routines for handling access requests from data subjects, to provide compliance also when exceeding the one-month time limit is permitted.

We find that there is a breach of Article 12(3) GDPR.

5. Judicial review

As we have informed earlier, this is a cross-border case. We have cooperated with other concerned supervisory authorities in the case handling. As mentioned, the Norwegian Data Protection Authority has, as lead supervisory authority in the case, a duty to hear all concerned supervisory authorities before a final decision is made.

In cross border cases, the Norwegian Privacy Appeals Board does not have competence to review the Norwegian Data Protection Authority's decisions, cf. Article 22(2) second sentence of the Personal Data Act.

The decision can be challenged before the courts. Each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them, cf. Article 78(1) GDPR. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established, cf. Article 78(1) GDPR. Court proceedings against the Norwegian Data Protection Authority shall be brought before Oslo District Court.¹⁰

¹⁰ Article 4-4(4) of the Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes, cf. Article 25 of the Personal Data Act.

6. Access to documents

The Norwegian Data Protection Authority has a duty of secrecy regarding the complainant's identity, cf. Article 24 of the Personal Data Act and Article 13 of the Public Administration Act. As a party to the case, you have the right to such information, cf. Article 13(b)(1)(1) Public Administration Act. You also have the right to access the documents in this case, cf. Article 18 of the Public Administration Act.

We also want to inform that all documents generally are subject to freedom of information requests, cf. Article 3 of the Norwegian Freedom of Information Act. If you are of the opinion that the document or parts of the document is exempt from public access, we ask you to give reasons for this.

Kind regards

Tobias Judin
Head of International

Guro Fiskvik Åsbø
Legal Adviser

This letter has electronic approval and is therefore not signed

Copy to: Complainant

Summary Final Decision Art 60

Complaint

Compliance order & Reprimand

EDPBI:LSA:OSS:D:2021:292

Background information

Date of final decision: 11 November 2021

Date of broadcast: 11 November 2021

LSA: NO

CSAs: FI, SE

Legal Reference: Article 5 (Principles relating to processing of personal data), Article 6 (Lawfulness of processing), 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 21 (Right to object)

Decision: Compliance order & Reprimand

Key words: Lawfulness of processing, Performance of contract, Direct marketing, Right to object

Summary of the Decision

Origin of the case

The complainant had been receiving direct marketing by e-mail without having the possibility to opt out upon registration of his e-mail address. He had objected to this processing in September 2018, yet he still received a direct marketing e-mail in November 2019. The complainant contacted the Data Protection Officer (DPO) of the controller on several occasions, and at times, his requests were answered in more than one month. When he requested the legal basis for processing his personal data, which he believed to be consent under Article 6(1)(a) GDPR, the DPO wrote in response that the legal basis was rather necessity for the performance of a contract pursuant to Article 6(1)(b) GDPR. Later, in another e-mail to the complainant, the DPO stated that the legal basis was Article 6(1)(f) GDPR for the purpose of marketing the bank's similar products, and Article 6(1)(b) GDPR for the purpose of marketing in relation to the customer benefit program.

Findings

The LSA established that there was no designated opt out possibility for marketing from the controller, but it was possible to 'approve' digital marketing via e-mail and SMS on the user page. As regards the lawfulness of the processing, the LSA reasoned that processing based on contractual performance must be objectively necessary, i.e. the controller should be able to demonstrate how the main subject-

matter of the specific contract with the data subject cannot be performed without the specific processing of the personal data in question. The processing of personal data for marketing purposes by the controller was not necessary for the performance of the contract related to the provision of a credit card service, and therefore, Article 6(1)(b) GDPR could not provide legal basis for the processing. The LSA found that the controller could not retroactively change the legal basis (from contractual performance to legitimate interest) after having commenced with the processing, as this leads to a lack of predictability for the data subject. In any event, a change in the legal basis for processing shall be communicated to the data subjects pursuant to Articles 12-14 GDPR.

Further, the LSA found that the controller breached Article 21(3) GDPR by continuing the processing of the complainant's personal data for direct marketing purposes after his objection to the controller's DPO. The provision of insufficient information on the legal basis of processing and the failure to inform the data subject on his right to object to processing for direct marketing by the controller constituted a breach of Articles 13(1), 12(1) and 21(4) GDPR. Finally, the controller's delays of over a month to respond to the complainant's requests, and without giving him reasons for these delays, constituted a breach of Article 12(3) GDPR.

Decision

The LSA issued a reprimand and ordered the controller to implement measures to ensure that personal data is no longer processed for direct marketing when so requested by data subjects and to ensure that data subject requests under Article 15-22 GDPR are answered within the time limits set in Article 12(3) GDPR.

NOVUM ØKONOMI AS
Havnegata 10
3040 DRAMMEN

Exempted from public access:
*Offl. § 13 jf. Popplyl. § 24 (1) 2.
pkt.*

Your reference

Our reference

20/03920-15

Date

14.01.2022

Decision to issue a reprimand

The Norwegian Data Protection Authority ("Datatilsynet", "we", "our") refer to our advance notification of a decision to issue a reprimand dated 4 November 2021 and earlier correspondence. We have not received comments to our advance notification of a decision to issue a reprimand by the deadline of 26 November 2021.

As mentioned in our request for information dated 7 May 2021, this is a cross-border case where we cooperate with other concerned national supervisory authorities in the case handling. Datatilsynet in Norway has been the lead supervisory authority in handling this case and this decision to issue a reprimand is taken after having heard all concerned supervisory authorities.

1. Decision to issue a reprimand

Datatilsynet has decided the following:

For:

- not informing the data subject about which steps you took after the data subject requested access to and erasure of personal data within a reasonable time frame in breach of Article 12 (3) of the General Data Protection Regulation ("GDPR"); and
- not providing the reasons for complying with the requests nor informing the data subject that they could submit a complaint to Datatilsynet in breach of Article 12 (4) of the GDPR,

Novum Økonomi AS («**Novum Økonomi**») is issued a reprimand.

Our legal basis for deciding to impose corrective measures is Article 58 (2) of the GDPR.

2. Subject of the complaint

We opened a case regarding Novum Økonomi based on a complaint from a data subject¹ in Poland. The complaint relates to how Novum Økonomi processes personal data. [REDACTED] [REDACTED] (the "Complainant") received a marketing email on 12 September 2018 for "3 D Perspective AS – Introduction of new contracts for the provision of accounting services in connection with new regulations regarding the protection of personal data (GDPR)". The email was sent from penneo@penneo.com to the Complainant's email address [REDACTED].

The Complainant reacted because he had not had anything to do with Penno AS ("Penno") previously. The Complainant therefore sent a complaint to the Polish Data Protection Authority stating that:

- He had never given consent to Penno to process his personal data;
- He did not receive any response from Penno after he asked them where they had obtained his personal data; and
- He did not receive any response from Penno when he requested to have his personal data erased.

3. Factual background

In 2019 the Danish Data Protection Agency was designated the leading supervisory authority because Penno is a Danish company and it was assumed that Penno was the data controller for the relevant processing, pursuant to Articles 60, 4 (7), 4 (16) and 4 (23) of the GDPR.

Through its correspondence with Penno, the Danish Data Protection Agency uncovered that Penno is a company that helps other businesses with digitalising processes regarding electronic signatures. Penno stated that they are only a data processor (pursuant to Article 4 (8)), and that they carry out work when their customers place an order with them. According to Penno, the data controller for the relevant processing activity was their customer Novum Økonomi. Furthermore, Penno stated that they only process personal data that the customer has actively inserted when using the software.

Penno has examined their systems and they could not find any information about the Complainant (i.e. email address or name) there. According to Penno, they had communicated with Novum Økonomi via telephone, and Novum Økonomi stated that the aforementioned email was sent to the Complainant by mistake because of human error. Penno has since deleted the Complainant's personal data.

As Novum Økonomi was data controller for the relevant processing activity, and it has its main business activities in Norway, Datatilsynet was designated as the new leading supervisory authority.

¹ The individual to whom the processed personal data can be linked

On 7 May 2021, Datatilsynet sent a request for information to you, Novum Økonomi, and received a response on 2 June 2021. You confirmed, among other things, that the aforementioned email was sent to the Complainant by mistake. You stated that it probably happened due to a typing error, so that the Complainant received the email instead of the intended customer. You have stated that this probably happened because the sender did not double-check the email address before sending.

Furthermore, you have stated that you had not obtained any personal data about the Complainant. You have also stated that you have not had access to his personal data and neither had any information about him that you could delete. Again, you highlighted that the Complainant has not been registered in your systems.

According to you, one of your employees, [REDACTED], contacted the Complainant by telephone in May 2019. She explained to the Complainant that he possesses the same name as one of Novum Økonomi's customers, and that this could be the explanation for how the email came to him instead of the customer. Ms [REDACTED] also apologised on behalf of Novum Økonomi and stressed that you never would have done anything actively to get the Complainant's email address.

Regarding Novum Økonomi's routines and measures for preventing such breaches, you have stated that according to your routines, active consent from the recipient is required when there is no previous relationship. This also applies if the email address is publicly available. Furthermore, you follow the industry standard "*KS Komplett*" which, among other things, concerns internal routines for outgoing emails. Regarding routines for ensuring the rights of the data subject or the customer according to Articles 15 to 21 of the GDPR, you have stated that you act in accordance with your trade association "*Regnskap Norge, KS Komplett*".

4. The applicable legal framework

4.1. About personal data, data controller and data processor

Personal data

Personopplysningsloven (The Norwegian Privacy Act) implements the GDPR in Norwegian law, and came into force on 20 July 2018. It follows from Article 4 (1) of the GDPR that 'personal data' means any information relating to an identifiable natural person, either directly or indirectly. 'Processing' of personal data means any operation or set of operations which is performed on personal data (for example collection or registration), pursuant to Article 4 (2) of the GDPR.

Data controller and data processor

The one who determines the purpose of and the means of the processing is the so-called data controller. The data controller can choose to have a so-called data processor, who processes the personal data on behalf of the data controller.

The full definitions of 'data controller' and 'data processor' follow from Article 4 (7) and (8) of the GDPR, pursuant to personopplysningsloven § 1.

4.2. Legal basis – lawful processing of personal data

The general principles for processing personal data follow from Article 5 (1) of the GDPR. Personal data shall be processed lawfully, fairly and in a transparent manner, pursuant to Article 5 (1) (a).

According to Article 5(2) of the GDPR, the data controller is responsible for ensuring and documenting that its processing complies with the general principles of article 5 (1).

Any processing of personal data must have a legal basis under Article 6 (1) of the GDPR to be lawful. A form of legal basis for the processing can be that the data subject has consented to the processing of personal data for one or more specific purposes (Article 6 (1) (a)).

Datatilsynet is not the competent authority for areas specifically regulated by markedsføringsloven (the Norwegian Marketing Act). According to the Norwegian Marketing Act § 15 (3), it is not necessary to get consent for marketing by electronic mail when there is already an existing customer relationship, under certain conditions.

Forbrukertilsynet (the Norwegian Consumer Agency) supervises whether organisations comply with the terms of the Norwegian Marketing Act. Nevertheless, organisations must also make sure that the processing of personal data is lawful according to the GDPR.

One of the legal bases provided for under Article 6(1)(a)-(f) is required in order to be able to lawfully process personal data.

4.3. Obligation to facilitate the rights of the data subject – the right of access and the right of erasure

Organisations must facilitate data subjects exercising their rights under the GDPR (Article 12 (2) of the GDPR). This means that organisations must allocate resources and have systems in place to consider requests from private individuals. For example, organisations must have resources and routines to handle requests for access to personal data according to Article 15 of the GDPR.

Data subjects have a right to **access** all personal data concerning them that the organisation processes (Article 15). It is possible to make some exceptions from the right to access under Article 15 (4) of the GDPR and The Norwegian Data Protection Act § 16.

Article 17 of the GDPR in some cases gives data subjects a right to **erasure** if certain conditions are met, and there is a corresponding duty for the organisation to erase their personal data. This includes, among other things, cases where a data subject withdraws their consent, if it is no longer necessary to process personal data for the purpose they were collected for, or if the personal data have been processed unlawfully.

4.4. Deadlines and such for responding to the data subject's request

When a data subject exercises their rights under Articles 15 to 22 of the GDPR, the organisation shall respond to the data subject without undue delay and in any event within one month of receipt of the request (Article 12 (3)). This deadline can be extended by two further months where necessary, but the organisation must then send the reasons for the delay within the deadline. The response shall include information about what measures have been taken.

Furthermore, it follows from Article 12 (4) of the GDPR that if the data controller does not take action at the request of a data subject, the data controller shall inform the data subject without delay and the latest within one month of receipt of the request of the reasons for not taking action. The data controller shall also inform the data subject they have a right to file a complaint with the supervisory authority and the right to seek a judicial remedy.

5. Datatilsynet's assessment

5.1. Regarding personal data, data controllers and data processors

Datatilsynet considers that the email address and name are personal data and that the incorrectly sent email is a processing of personal data. In addition, Datatilsynet finds on the balance of probabilities that Novum Økonomi is the data controller and Penno is the data processor for this processing activity, pursuant to Article 4 (7) and (8) of the GDPR.

5.2. Legal basis – lawful processing of personal data

Novum Økonomi writes in their statement dated 2 June 2021 that the email sent to the Complainant was sent due to a (human) error. Datatilsynet therefore finds on the balance of probabilities that the processing of the personal data, i.e. sending marketing material by email to the Complainant, happened without a legal basis according to Article 6 (1) of the GDPR and without being in accordance with the general principles given in Article 5 (1) of the GDPR.

Datatilsynet therefore concludes that Novum Økonomi processed the Complainant's personal data in an illegal manner, pursuant to Articles 6 (1) and 5 (1) of the GDPR.

However, Datatilsynet believes that the threshold for giving a reprimand for these conditions has not been met. This is because it was a one-time incident and the email sending happened as a result of human error (and not system failure). The breach has further not had any major privacy consequences for the Complainant.

5.3. Obligation to facilitate the data subject's rights – access and erasure

As to the question of breach regarding the Complainant's request for access and erasure, Datatilsynet cannot find any breach of Article 15 (1), (3) or Article 17 (1) of the GDPR.

This is because the email address was erased from both Penno's and Novum Økonomi's systems and databases, so that neither the data controller nor the data processor processes the Complainant's personal data anymore. There is thus no personal data about the complainant to erase.

Datatilsynet also notes that the complainant has received information regarding how their e-mail address came into being with the businesses, i.e. that it was a typographical error in the system.

5.4. Deadlines and such for responding to the data subject's requests

Datatilsynet cannot see that Novum Økonomi has given the Complainant information about measures taken based on his request for access/erasure of 12 September 2018 without undue delay², and at the latest within one month after the request was received (Article 12 (3)). We can further not see that Novum Økonomi has given the Complainant any information about the delay or its reasons within one month.

The Complainant was not contacted by Novum Økonomi, represented by [REDACTED], until May 2019. [REDACTED] then informed him that the email had been sent to him by mistake and that the company had not collected any information about him. In the phone call, it was also informed that the company no longer processed any personal data about the Complainant.

Furthermore, Datatilsynet cannot see that Novum Økonomi informed the Complainant about their right to file a complaint with the supervisory authority and the right to seek a judicial remedy (Article 12 (4)).

Novum Økonomi did not inform the Complainant about which steps were taken, nor about which steps could not be taken, why, and about the right to make a complaint or seek judicial remedy, by the company after the Complainant had requested access and erasure within the deadline mentioned. Based on this, Datatilsynet finds a breach of Article 12 (3) and (4) of the GDPR.

Datatilsynet issues a reprimand due to the severity of the breach, and Datatilsynet finds on the balance of probabilities that Novum Økonomi does not have routines in place/followed its routines for facilitating that the data subject can exercise his rights (Article 12 (2)). Datatilsynet places particular emphasis on the fact that it took about eight months from when the Complainant first got in touch with Novum Økonomi with his request for access and erasure, until he received this information from Novum Økonomi.

6. Final remarks

² According to the Complainant's letter with clarifications to the Danish Data Protection Agency dated 17 March 2020, the Complainant sent an email to the email address info@novumc.com on 12 September 2018. This should be the correct email address to send a request to. In addition, the Complainant followed up with an email to both info@novumc.com and penneo@penneo.com on 11 May 2019, since the Complainant had never received any response from Novum Økonomi in the first mentioned email.

6.1. Ability to appeal this decision

In cross-border cases, the Norwegian Privacy Appeals Board does not have standing to overturn Datatilsynet's decisions pursuant to personopplysningsloven Section 22 second paragraph.

This decision can be appealed to the Norwegian courts. All physical and legal persons shall have the right to an efficient judicial remedy against a legally binding decision of a supervisory authority concerning them pursuant to Article 78 (1) of the GDPR. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established pursuant to Article 78 (3) of the GDPR. Proceedings against Datatilsynet shall be brought before Oslo City Court.³

6.2. Public access, other access and confidentiality

We want to inform you that all documents generally are subject to freedom of information requests, pursuant to offentlighetsloven § 3 (the Norwegian Freedom of Information Act). If you are of the opinion that the document is, or parts of the document are, exempt from public access we ask you to justify this.

Datatilsynet has a duty of confidentiality about who complained to us, and about the complainant's personal situation. The duty of confidentiality follows from, among others things, The Norwegian Data Protection Act § 24 and the Norwegian Public Administration Act § 13. As a party in the case you can still be made aware of such information by Datatilsynet, cf. the Norwegian Public Administration Act § 13 b (1) (1). You also have the right to access the case documents, cf. the Norwegian Public Administration Act § 18.

We draw attention to the duty of confidentiality you have when Datatilsynet gives you information about the Complainant's identity, personal situation or other identifying data, and that you may only use this information to the extent it is necessary to look after your own self-interests in this case, cf. the Norwegian Public Administration Act § 13 b (2). We also point out that violation of the duty of confidentiality can be punished according to straffeloven (the Norwegian Criminal Code) Section 209.

Should you have questions, you may contact Sebastian Forbes by telephone on 22 39 69 49.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes

³ Law of 17 June 2005 no. 90 on mediation and court proceedings in civil disputes (the Dispute Act) § 4-4 (4), pursuant to Section 25 of the Norwegian Data Protection Act.

Legal Advisor

Copy to: The Complainant

MOWI ASA
Postboks 4102 Sandviken
5835 BERGEN

Your reference

Our reference

21/03656-12

Date

26.04.2022

Reprimand and Compliance Order - Mowi ASA

1. Introduction

The Norwegian Data Protection Authority (“Datatilsynet”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“GDPR”)¹ with respect to Norway.

On 2 March 2022, we notified Mowi ASA (“Mowi”, “you”, “your”, “the company”) of our intention to issue a reprimand and compliance order for having violated Article 14 GDPR.

On 23 March 2022, Mowi acknowledged our advance notification without raising any arguments to contest the conclusions or factual descriptions laid down in the advance notification.

On 24 March 2022, Datatilsynet submitted a draft decision—which essentially reproduced the above advance notification—to the other supervisory authorities concerned in accordance with Article 60(3) GDPR. None of the other supervisory authorities concerned expressed a relevant and reasoned objection to the draft decision within four weeks after having been consulted by Datatilsynet.

Thus, the present decision is adopted in conformity with the advance notification we sent to Mowi and the draft decision we submitted to the other supervisory authorities concerned.

2. Decision

Pursuant to Article 58(2)(b) GDPR, Datatilsynet issues a reprimand against Mowi for:

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2018] L 119/1.

- having infringed Article 14 GDPR by failing to provide all of the relevant information required therein.

Pursuant to Article 58(2)(d) GDPR, Datatilsynet orders Mowi to:

- take measures to ensure that data subjects (including Mowi's shareholders whose personal data are processed pursuant to the Norwegian Public Limited Liability Companies Act)² are provided with all of the information required by Article 14 GDPR, including by amending its privacy policy as necessary. Such information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Mowi shall notify the measures taken for complying with this order to Datatilsynet within four weeks after having received the present decision.

3. Factual Background

On 14 April 2021, a data subject residing in Germany who owned shares in Mowi was notified by his German bank that Mowi had requested his personal data from the bank pursuant to a Norwegian law (i.e., the Norwegian Public Limited Liability Companies Act, § 4-10).³

After having received such a notification from his bank, the data subject wrote an email to info@mowi.com (i.e., the email address provided in Mowi's privacy policy in effect at the time)⁴ to exercise his right of access under Article 15 GDPR on 26 July 2021.⁵ On 2 September 2021, the data subject sent the company a reminder of his request to the same email address,⁶ but he received no response from Mowi.⁷

On 4 October 2021, the data subject sent a complaint against Mowi to Datatilsynet, in which he essentially claimed that Mowi failed to comply with: (1) Article 14 GDPR, as the company failed to inform him about the purposes for which his personal data have been collected; and (2) Articles 12(3) and 15 GDPR, as the company did not respond within the applicable deadline to the access requests that the complainant sent to Mowi. The complainant also asked that Datatilsynet order Mowi to respond to the request at hand pursuant to Article 58(2)(c) GDPR.⁸

On 2 December 2021, Datatilsynet sent a letter to Mowi asking the company to provide its views on the issues raised by the complainant,⁹ and we received the company's response on 23 December 2021.¹⁰

² Norwegian Public Limited Liability Companies Act ("Lov om allmennaksjeselskaper (allmennaksjeloven)", LOV-1997-06-13-45).

³ See complaint dated 4 October 2021.

⁴ See: <<https://web.archive.org/web/20210814074115/https://mowi.com/about/privacy-policy/>>. All web links provided in the present letter have been last accessed on 24 March 2022.

⁵ See Annex I to the complaint dated 4 October 2021.

⁶ See Annex II to the complaint dated 4 October 2021.

⁷ See complaint dated 4 October 2021.

⁸ Ibid.

⁹ See Krav om redegjørelse - Mowi ASA (ref: 21/03656-2).

¹⁰ See DATATILSYNETS KRAV OM REDEGJØRELSE – MOWI ASA (ref: 514012) (hereinafter "Mowi's Reply to Datatilsynet").

In its reply to Datatilsynet, Mowi acknowledged that it did not respond to the complainant's access request.¹¹ However, it stated that this was due to the fact that both emails from the complainant ended up in the spam folder of the company's email inbox.¹² Mowi also stated that it would answer the data subject's request after having responded to Datatilsynet's inquiry.¹³

Further, Mowi acknowledged that it did not provide any information on the processing at issue in the present case, neither through its privacy policy nor directly to the data subject, pursuant to Article 14 GDPR.¹⁴ However, it took the view that it was not required to provide any information on such processing, as it was entitled to rely on the exceptions set out in Article 14(5)(a) and (c) GDPR.¹⁵

On 3 January 2022, Mowi sent the following response to the complainant:

[...] *We would like first to express our sincere apologies for not responding to your access request within the deadline. We have had difficulties with extensive amounts of spam and phishing attempts towards this inbox, and your requests were caught in the clutter folder and unfortunately not detected as a legitimate claim through our regular routines and procedures. This is meant only as an explanation and not an excuse for our delay in responding. We can assure you that proper measures have been taken to avoid this happening again. We have established a new privacy inbox in relation our privacy policy on mowi.com, and have strengthened our follow-up procedures.*

Your request to Mowi was, with reference to your email of July 2021, prompted by our supplier Nasdaq's request to your holding bank for the disclosure of your data, pursuant to section 4-10 of the Norwegian PLC Act. You raised the question of why this request was made by Nasdaq and on this background submitted an access request.

We will in the following explain the background for Mowi's request, give an overview of what is requested, and the legal foundation for our request.

NASDAQ OMX Corporate Solutions International Limited) ("Nasdaq") is engaged by Mowi to provide Share Register Analysis Services. The processing of information gathered for the share register is governed through an Agreement and relevant supporting documents for processing of personal information. Nasdaq is registered in the UK and the transfer of personal data to UK is governed by Standard Contractual Clauses entered into between Mowi and Nasdaq. Specifically in relation to the Service, Nasdaq on behalf of Mowi ASA reaches out to various Custodian banks to request shareholder information pursuant to the Norwegian Public Limited Companies Act and GDPR regulation Article 6(1)(f).

¹¹Ibid., answer to Q.5.

¹²Ibid., answer to Q.7.

¹³Ibid., answer to Q.5.

¹⁴Ibid., answer to Q.4 (stating: "Vi erkjenner at Mowi selv ikke har gitt informasjon om den aktuelle behandlingen i sin personvernerklæring. Det har heller ikke vært direkte kommunikasjon med den registrerte.").

¹⁵Ibid.

The information collected by Nasdaq is simply the name of the shareholder. Further information that may be collected is address, country and number of shares held.

The purpose of collecting the information is Mowi's need to know who the shareholders are, pursuant to section 4-10 of the Norwegian PLC Act. Mowi uses this information to follow up investors and share relevant information about the corporation. As a listed corporation, our investor relations department meet with a lot of investors throughout the year. A shareholder overview of relevant investors is therefore needed to maintain proper investor relations services.

According to the Agreement with Nasdaq, Mowi receives from Nasdaq information on shareholders holding 10,000 shares or more. This means that Mowi has not received specific information about you as a shareholder, but rather aggregated information of Custodian banks holding shares for smaller shareholders below the set threshold.

Nasdaq holds the information as long as it is needed, but never longer than 5 years, whichever is first.

You have the right to request rectification, erasure, and restriction of the personal data we process on you, and you may object to such processing. As you are aware, you also have the right to lodge a complaint with the supervisory authority (Norwegian Data Authorities). [...].¹⁶

On 4 January 2022, the complainant informed Datatilsynet that it found the above response to be satisfactory.¹⁷

On 2 March 2022, Datatilsynet notified Mowi of our intention to issue a reprimand and compliance order against the company for having violated Article 14 GDPR.¹⁸ In that letter, we outlined the factual background of the present case;¹⁹ we described the legal and factual grounds on which we based our competence to handle the case as a lead supervisory authority under Article 56 and Chapter VII GDPR;²⁰ we explained why—in our view—Mowi had violated Article 14 GDPR, and the company's arguments regarding the applicability of the exceptions in Article 14(5)(a) and (c) GDPR are to be rejected;²¹ and we described the main flaws in Mowi's transparency documentation and routines that the company must remedy.²²

¹⁶ See Mowi's email to the complainant dated 3 January 2022 (hereinafter "Mowi's Response to the Complainant").

¹⁷ See email from the complainant dated 4 January 2022.

¹⁸ See Advance Notification – Reprimand and Compliance Order – Mowi ASA (ref: 21/03656-9).

¹⁹ Ibid., section 3.

²⁰ Ibid., section 5.

²¹ Ibid., section 6.2.

²² Ibid.

On 23 March 2022, Mowi sent us a letter in which the company acknowledged our advance notification.²³ In that latter, Mowi did not raise any arguments to contest the conclusions or factual descriptions laid down in our advance notification. However, the company informed Datatilsynet that Mowi is in the process of updating its privacy policy, internal documentation and routines.²⁴

4. Legal Background

4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

[...] applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Moreover, Article 3(1) GDPR provides that the Regulation:

[...] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

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

Pursuant to Article 4(2) GDPR:

“processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

²³ See DPA’S ADVANCE NOTIFICATION – REPRIMAND AND COMPLIANCE ORDER – MOWI ASA (ref: 514012).

²⁴ Ibid.

Pursuant to Article 4(7) GDPR:

“controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Pursuant to Article 4(9) GDPR:

“recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

4.3. Obligations Regarding Information and Access to Personal Data

Article 14 GDPR establishes which information is to be provided by a controller where personal data have not been obtained from the data subjects. In particular, Article 14(1) to (4) provides that:

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

- (a) *the identity and the contact details of the controller and, where applicable, of the 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 basis for the processing;*
- (d) *the categories of personal data concerned;*
- (e) *the recipients or categories of recipients of the personal data, if any;*
- (f) *where applicable, that the controller intends to transfer personal data to a recipient in 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 to obtain a copy of them or where they have been made available.*

In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a) *the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*
- (b) *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
- (c) *the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;*
- (d) *where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
- (e) *the right to lodge a complaint with a supervisory authority;*
- (f) *from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;*
- (g) *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.*

The controller shall provide the information referred to in paragraphs 1 and 2:

- (a) *within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;*
- (b) *if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or*
- (c) *if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.*

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

However, Article 14(5) establishes certain exceptions to the above information obligations:

Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

[...]

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; [...]

Further, Article 15 GDPR reads:

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.*

Furthermore, Article 12(1) to (4) GDPR provides 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.*

4.4. Competence, Tasks and Powers of Supervisory Authorities under the GDPR

Pursuant to Article 55(1) GDPR:

Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Further, Article 56(1) reads as follows:

Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

The term “main establishment” is defined in Article 4(16) GDPR as follows:

“*main establishment*” means:

- (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 of personal data 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; [...].*

The term “cross-border processing” is defined in Article 4(23) as follows:

“*cross-border processing*” means either:

- (a) *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
- (b) *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

Pursuant to Article 58(2) GDPR:

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

- (a) *to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*
- (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;*

- (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;
- (e) to order the controller to communicate a personal data breach to the data subject;
- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- (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;
- (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

4.5. EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area (“EEA”) Agreement by means of Decision of the EEA Joint Committee No 154/2018 (“EEA Joint Committee Decision”).²⁵

Article 1(b) of the EEA Joint Committee Decision provides that:

[...] the terms “Member State(s)” and “supervisory authorities” shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.

²⁵ Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.²⁶ The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet's Competence

Mowi is one of the largest seafood companies in the world. It has its headquarter in Norway, but has operations in at least 25 countries, including Belgium, Czech Republic, France, Germany, Ireland, the Netherlands, Italy, Poland, Spain, and Sweden. Moreover, Mowi is listed on the Oslo Stock Exchange (OSE) and its share also trades on the US OTC market.²⁷ Therefore, it has shareholders in several EU/EEA countries, including in Germany (where the complainant resides).

Thus, Mowi has several establishments in the EU/EEA, including in Norway, and in the context of the activities of these establishments it processes personal data, including personal data of its shareholders. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of its shareholders (including the complainant) in accordance with § 4-10 of the Norwegian Public Limited Liability Companies Act, Mowi qualifies as a controller (within the meaning of Article 4(7) GDPR), as it is Mowi that decide(d) to collect and process shareholder information—through its processor NASDAQ OMX Corporate Solutions International Limited—to “follow up investors and share relevant information about the corporation”.²⁸

As Mowi has a main establishment (within the meaning of Article 4(16) GDPR) in the EEA and its processing of shareholder information is cross-border (within the meaning of Article 4(23) GDPR), the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that Mowi’s main establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR.

6. Datatilsynet's Assessment

6.1. Mowi’s Failure to Respond to the Complainant’s Access Request

Under Article 12(3) GDPR, controllers are required to respond to access requests submitted pursuant to Article 15 GDPR “without undue delay and in any event within one month of receipt of the request.” However, in exceptional circumstances, that period may be extended by two further months.

²⁶ Act No 38 of 15 June 2018 relating to the processing of personal data (“personopplysningsloven”).

²⁷ See: <<https://mowi.com/>>.

²⁸ See Mowi’s Reply to Datatilsynet; Mowi’s Response to the Complainant.

In the present case, Mowi has acknowledged that it failed to respond to the complainant's access request within the above deadline.²⁹ However, Mowi stated that this was due to the fact that both emails from the complainant ended up in the spam folder of the company's email inbox.³⁰

Under Article 12(2) GDPR, controllers have an obligation to "facilitate the exercise" of the data subject right under Article 15 GDPR. This entails—among other things—that controllers should take adequate technical and organizational measures to ensure that they can receive and handle in a timely manner the access requests they receive from data subjects. In the words of the European Data Protection Board (EDPB):

*The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject.*³¹

This means that, although controllers remain free to decide which specific communication channel should be used for submitting access requests, they must ensure that the communication channel they implement is easy to use and effective. Thus, if a controller decides to receive access requests via email, it must make sure that the email account it uses for this purpose implements state-of-the-art anti-spam protection—which does not treat legitimate access requests as spam—and/or that it monitors the spam folder on a regular basis to identify the presence of possible legitimate access requests. Effective anti-spam solutions (e.g., CAPTCHA solutions) do exist and should be adequately considered by the controller, in accordance with its accountability obligations under the GDPR.³²

In the present case, Mowi's anti-spam solution failed to "facilitate" the exercise of the right under Article 15 GDPR, in breach of Article 12(2) GDPR, as it treated a legitimate access request as spam twice, leading to such a request remaining unanswered for over 5 months.

Nonetheless, we consider such an infringement to be minor,³³ for the following reasons:

- It appears to have affected a single data subject who was eventually satisfied with the delayed reply it received from Mowi;³⁴
- To date, Datatilsynet has not received any other complaints concerning Mowi's compliance with Articles 12(2) and 15 GDPR; and

²⁹ Ibid.

³⁰ Ibid.

³¹ EDPB, Guidelines 01/2022 on data subject rights - Right of access (Version 1.0, Adopted on 18 January) (hereinafter "EDPB Guidelines on the Right of Access"), p. 2.

³² Arts. 5(2) and 24 GDPR.

³³ Cf. rec. 148 GDPR.

³⁴ See Mowi's Reply to Datatilsynet, answer to Q.7.

- After Datatilsynet's inquiry, Mowi created a new email address to be used for sending access requests, which according to the company has enhanced filters for spam and phishing.³⁵

In light of the above, we find that—in the present case—it is not warranted to issue any corrective measures for this infringement, and considers the matter concerning Mowi's failure to reply to the complainant's access request to be amicably settled.³⁶ However, this is without prejudice to the possibility of opening future inquiries to verify whether the new email account set up by Mowi enables the company to comply with Articles 12(2) and 15 GDPR.

6.2. Mowi's Failure to Comply with Article 14 GDPR

In the present case, Mowi acknowledged that it did process—through its processor NASDAQ OMX Corporate Solutions International Limited—the personal data of the complainant,³⁷ as well as the personal data of other shareholders,³⁸ under the Norwegian Public Limited Companies Act. It also stated that such personal data were and are normally obtained from “various Custodian banks”,³⁹ and not directly from the individual shareholders.

Further, Mowi acknowledged that it did not provide any information on the processing of shareholder information pursuant to the Norwegian Public Limited Companies Act, neither directly to the data subject nor in its privacy policy.⁴⁰ Indeed, Mowi's privacy policy in effect at the time of the complaint simply stated:

This privacy notice applies for processing of personal data carried out by Mowi for any persons not employed by Mowi.

[...]

Mowi collects personal data by/from direct contact with you, online forms, third parties, newsletters etc.

[...]

*The legal basis and the purpose for Mowi's processing of your personal data is based on your consent, and direct mail.*⁴¹

³⁵ Ibid. (stating: “Mowi har [...] gjort tiltak for at dette ikke skal skje igjen. Det er opprettet en ny epostadresse for slike henvendelser (privacy@mowi.com) med forbedrede filtre for spam og phishing”).

³⁶ Cf. rec. 131 GDPR.

³⁷ Mowi's Reply to Datatilsynet, answers to Q.1.

³⁸ Mowi's Response to the Complainant (stating: “Nasdaq on behalf of Mowi ASA reaches out to various Custodian banks to request shareholder information pursuant to the Norwegian Public Limited Companies Act”).

³⁹ Ibid.

⁴⁰ Mowi's Reply to Datatilsynet, answer to Q.4 (stating: “Vi erkjenner at Mowi selv ikke har gitt informasjon om den aktuelle behandlingen i sin personvernerklæring”).

⁴¹ See: <<https://web.archive.org/web/20210814074115/https://mowi.com/about/privacy-policy/>>.

However, in its first reply to Datatilsynet, Mowi took the view that it was not required to provide any information on the processing at hand pursuant to Article 14(5)(a) and (c) GDPR. In this regard, Mowi argued:

The complainant has bought shares in Mowi via his bank, where the bank acts as the custodian of the shareholding. It is assumed that in this connection the complainant has become aware that information about him is disclosed to the company in which he buys shares. This must also be seen in connection with the Public Limited Liability Companies Act §4-10 fourth paragraph where it is explicitly stated that the company has an unconditional right to receive information from the custodian about who is the underlying owner of the shares covered by the custodian assignment, and how many shares each individual owns. It must be assumed that a shareholder who uses a custodian is familiar with this provision. Mowi is therefore of the opinion that no further information is necessary, cf. Article [sic] 15 a) and c) of the GDPR. (our translation)⁴²

In our view, Mowi's arguments regarding the applicability of the exceptions in Article 14(5)(a) and (c) in the context at issue in the present case are to be rejected. This is for the reasons outlined below.

First, as noted by the EDPB, the exceptions in Article 14(5) should be interpreted and applied narrowly.⁴³ Thus, any broad derogation from the information obligations laid down in Article 14—such as the one that Mowi advocates for—should be rejected.

Secondly, Article 14(5)(a) sets out an exception to the information obligations in Article 14, which applies “where and insofar as” the data subject already has the information. Thus, this exception applies only if the controller can “demonstrate (and document) what information the data subject already has, how and when they received it”.⁴⁴ Thus, to rely on this exception, it is not sufficient to “assume” that a data subject has received the information required under Article 14, as Mowi did in this case. Indeed, Mowi did not produce any evidence that the complainant’s

⁴² Mowi's Reply to Datatilsynet, answer to Q.4 (stating in Norwegian: “Klageren har kjøpt aksjer i Mowi via sin bank, hvor banken opptrer som forvalter av aksjeposten. Det forutsettes at klager i den forbindelse har blitt kjent med at opplysninger om ham formidles til selskapet han kjøper aksjer i. Dette må også sees i sammenheng med allmennaksjeloven §4-10 fjerde avsnitt hvor det uttrykkelig fremkommer at selskapet har en ubetinget rett til å få opplyst fra forvalteren hvem som er underliggende eier av de aksjer forvalteroppdraget omfatter, og om hvor mange aksjer hver enkelt eier. Det må forutsettes at en aksjonær som benytter forvalter også er kjent med denne bestemmelsen. Mowi er derfor av den oppfatning at det ikke er nødvendig med ytterligere informasjon, jfr. personvernforordningens artikkel [sic] 15 a) og c). Vi erkjenner at Mowi selv ikke har gitt informasjon om den aktuelle behandlingen i sin personvernerklæring. Det har heller ikke vært direkte kommunikasjon med den registrerte. På bakgrunn av saken vil vi gjennomgå våre rutiner for informasjon for å vurdere om slik informasjon skal gis direkte, eller på annen hensiktsmessig måte”). Note that Mowi has acknowledged that in this passage it intended to refer to Article 14(5)(a) and (c), and not to Article 15. See Mowi's email to Datatilsynet dated 23 December 2021.

⁴³ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, Adopted on As last Revised and Adopted on 11 April 2018) (hereinafter “Transparency Guidelines”), para. 57. Such guidelines have been endorsed by the EDPB. See EDPB, Endorsement 1/2018 (25 May 2018).

⁴⁴ Ibid., para. 56.

bank provided him with any information on Mowi’s processing of his personal data; it just assumed it.⁴⁵

Further, the exception in Article 14(5)(a) only applies “insofar as” the data subject has the information required in Article 14(1) to (2). This means that this exception applies only with respect to the specific information that the data subject actually has. However, the controller must supplement that information to ensure that the data subject has a *complete set* of the information listed in Article 14(1) to (2).⁴⁶ In this regard, it should be noted that at least some—if not all—of the information listed in Article 14(1) to (2) was not available to the complainant. For instance, the complainant was not aware at least of the following:

- The legal basis for the processing under the GDPR (Article 14(1)(c)). According to Mowi, the relevant legal basis was Article 6(1)(f).⁴⁷ Nonetheless, Mowi’s privacy policy only mentioned consent as a legal basis for the “processing of personal data carried out by Mowi for any persons not employed by Mowi” (emphasis added),⁴⁸ and the Public Limited Liability Companies Act does not provide any information on the legal basis to be relied on under the GDPR for processing shareholder information.
- The recipients or categories of recipients of the personal data (Article 14(1)(e)). In its replies to Datatilsynet and the complainant, Mowi stated that shareholder information is disclosed to NASDAQ OMX Corporate Solutions International Limited,⁴⁹ although Mowi’s privacy policy stated that “personal data are not to be disclosed to third parties unless Mowi is obliged to disclose such information”,⁵⁰ and no such obligation exists under the Norwegian Public Limited Liability Companies Act with respect to third parties such as NASDAQ.
- Information on international data transfers and suitable safeguards (Article 14(1)(f)). In its reply to the complainant, Mowi stated that “Nasdaq is registered in the UK and the transfer of personal data to UK is governed by Standard Contractual Clauses entered into between Mowi and Nasdaq”.⁵¹ However, Mowi’s privacy policy stated: “Mowi will not transfer your personal data to third countries outside the EU/EEA unless you have you have expressly been informed [and consented to] otherwise”.
- The period for which the personal data will be stored (Article 14(2)(a)). In its reply to the complainant, Mowi stated: “Nasdaq holds the information as long as it is needed, but never longer than 5 years, whichever is first.” However, no such information was

⁴⁵ Mowi’s Reply to Datatilsynet, answer to Q.4 (stating: “Det *forutsettes* at klager …”, emphasis added).

⁴⁶ Transparency Guidelines, para. 56.

⁴⁷ Mowi’s Reply to Datatilsynet, answer to Q.2.

⁴⁸ See: <<https://web.archive.org/web/20210814074115/https://mowi.com/about/privacy-policy/>>.

⁴⁹ Mowi’s Reply to Datatilsynet, answer to Q.3; Mowi’s Response to the Complainant. It should be noted that processors qualify as recipients under Article 4(9) GDPR. See Transparency Guidelines, page 37.

⁵⁰ See: <<https://web.archive.org/web/20210814074115/https://mowi.com/about/privacy-policy/>>.

⁵¹ Mowi’s Response to the Complainant.

mentioned in Mowi’s privacy policy,⁵² nor does the Norwegian Public Limited Liability Companies Act regulate such a retention period.

Thirdly, the exception in Article 14(5)(c) applies when the following two conditions are met: (1) “obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject”; and (2) such law “provides appropriate measures to protect the data subject’s legitimate interests”.

As for the first condition, the EDPB noted that:

Such a law must directly address the data controller and the obtaining or disclosure in question should be mandatory upon the data controller. Accordingly, the data controller must be able to demonstrate how the law in question applies to them and requires them to either obtain or disclose the personal data in question.⁵³ (emphasis added)

In this regard, it should be noted that—as acknowledged by Mowi⁵⁴—§ 4-10 of the Norwegian Public Limited Liability Companies Act provides for a “right” which enables Mowi to obtain shareholder information; it does not *require* Mowi to obtain such information.⁵⁵ Indeed, Mowi claimed that the legal basis for processing shareholder information pursuant to the Norwegian Public Limited Liability Companies Act is Article 6(1)(f), and not Article 6(1)(c) GDPR. Thus, the first condition laid down in Article 14(5)(c) is not met in the present case.

For completeness purposes, it should be noted that also the second condition set out in Article 14(5)(c) is not met in the present case, as Mowi failed to demonstrate that the Norwegian Public Limited Liability Companies Act provides appropriate measures to protect the data subjects’ (i.e., the shareholders’) legitimate interests and how Mowi complied with such appropriate measures. As noted by the EDPB:

While it is for Union or Member State law to frame the law such that it provides “appropriate measures to protect the data subject’s legitimate interests”, the data controller should ensure (and be able to demonstrate) that its obtaining or disclosure of personal data complies with those measures.⁵⁶

In any event, it should be noted that, even when a controller is able to rely on the exception in Article 14(5)(c):

⁵² See: <<https://web.archive.org/web/20210814074115/https://mowi.com/about/privacy-policy/>>.

⁵³ Transparency Guidelines, para. 66.

⁵⁴ Mowi’s Reply to Datatilsynet, answer to Q.4 (stating in Norwegian: “[...] allmennaksjeloven §4-10 fjerde avsnitt hvor det uttrykkelig fremkommer at selskapet har en ubetinget rett til å få opplyst fra forvalteren hvem som er underliggende eier av de aksjer forvalteroppdraget omfatter, og om hvor mange aksjer hver enkelt eier”; emphasis added).

⁵⁵ Norwegian Public Limited Liability Companies Act, § 4-10, which reads in Norwegian: “Dersom selskapet eller en offentlig myndighet krever det, plikter forvalteren å gi opplysninger om hvem som eier de aksjer forvalteroppdraget omfatter, og om hvor mange aksjer hver enkelt eier”.

⁵⁶ Transparency Guidelines, para. 66.

*the data controller should make it clear to data subjects that it obtains or discloses personal data in accordance with the law in question, unless there is a legal prohibition preventing the data controller from doing so.*⁵⁷

Fourthly, Mowi’s privacy policy in effect at the time of the complaint would have led essentially any data subject to believe that the “processing of personal data carried out by Mowi for any persons not employed by Mowi,” including “personal data by/from [...] third parties” would exclusively take place on the basis of the data subject’s consent, for advertising purposes (“The legal basis and the purpose for Mowi’s processing of your personal data is based on your consent, and direct mail”) (emphasis added).⁵⁸ Thus, any data subject/shareholder who would have reasonably relied on the information provided in Mowi’s privacy policy would have most likely concluded that Mowi did not process personal data for any other purpose or legal basis. This kind of incomplete and misleading communication is incompatible with the transparency principle set out in Article 5(1)(a) GDPR.

In this regard, it should be noted that—after the opening of Datatilsynet’s inquiry—Mowi partially amended its privacy policy on 20 December 2021, and its privacy policy no longer refers exclusively to consent as a legal basis for Mowi’s processing activities.⁵⁹

In light of the above, the information obligations laid down in Article 14 GDPR were applicable to Mowi. Thus, Mowi violated Article 14, as it failed to provide all of the information required under that Article within one month after having obtained the complainant’s personal data from his bank.⁶⁰

In our view, such a violation warrants the imposition of a reprimand pursuant to Article 58(2)(b) GDPR. This is because the complainant was eventually provided with the information he wished to obtain—albeit with a considerable delay—and hence the detriment suffered by the complainant was minimal in practice, which is confirmed by the fact that the complainant was satisfied with Mowi’s delayed reply. However, Mowi’s approach with regard to its obligations under Article 14 entails that similar violations have likely taken place with respect to other shareholders and may reoccur in the future.⁶¹ Thus, the adoption of a corrective measure appears to be appropriate in this case, in particular to discourage future similar instances of non-compliance, and uphold the data protection rights of other shareholders.

In addition, while the scope of our inquiry did not cover a full review of Mowi’s privacy policy in effect at the time of the present decision, we note that the privacy policy as last amended in December 2021 appears to be insufficient to comply with the transparency obligations that Mowi has under the GDPR. For instance:

⁵⁷ Ibid.

⁵⁸ See: <<https://web.archive.org/web/20210814074115/https://mowi.com/about/privacy-policy/>>. The Norwegian version of the privacy policy stated, more clearly: “rettsgrunnlaget for Mowis behandling av personopplysningene dine er ditt samtykke, og formålet er utsendelse av reklame”.

⁵⁹ See: <<https://mowi.com/about/privacy-policy/>>.

⁶⁰ Art. 14(3)(a) GDPR.

⁶¹ Note that Mowi stated that “Nasdaq on behalf of Mowi ASA reaches out to various Custodian banks to request shareholder information pursuant to the Norwegian Public Limited Companies Act” (emphasis added). See Mowi’s Response to the Complainant.

- Under “legal basis and purpose”, Mowi’s privacy policy—which applies to the “processing of personal data carried out by Mowi for any persons not employed by Mowi” (emphasis added)—simply replicates the wording of Article 6(1) GDPR without clarifying the actual purposes of, and legal basis for, the specific data processing activities envisaged by Mowi so as to allow the data subject to assess, on the basis of his or her own situation , what legal basis/purpose(s) apply.⁶² The privacy policy merely states:

“Mowi may process Personal Data relating to Users if one of the following applies:

Users have given their consent for one or more specific purposes. Note: Under some legislation Mowi may be allowed to process Personal Data until the User objects to such processing (“opt-out”), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;

provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;

processing is necessary for compliance with a legal obligation to which Mowi is subject;

processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in Mowi;

processing is necessary for the purposes of the legitimate interests pursued by Mowi or by a third party.

In any case, Mowi will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.”⁶³

- With regard to international data transfers, the privacy policy states: “Mowi will not transfer your personal data to third countries outside the EU/EEA unless you have you have expressly been informed [and consented to] otherwise”,⁶⁴ although Mowi has acknowledged that it transfers at least shareholder information to NASDAQ in the UK, without consent.
- With regard to data retention periods, the privacy policy states that “Personal Data shall be processed and stored for as long as required by the purpose they have been collected for,”⁶⁵ without providing any additional information that would enable the data subject

⁶² Cf. Transparency Guidelines, page 9.

⁶³ See: <<https://mowi.com/about/privacy-policy/>>.

⁶⁴ Ibid.

⁶⁵ Ibid.

to assess, on the basis of his or her own situation, what the retention period will be for specific data/purposes.⁶⁶

The examples provided above show that—if Mowi’s privacy policy is at least partially intended to provide the information required by Article 14 GDPR, as it seems to be the case, given that the privacy policy states that “Mowi collects personal data by/from direct contact with you, online forms, third parties, newsletters etc.” (emphasis added)—to ensure full compliance with Article 14 Mowi not only needs to make sure that its shareholders are given the necessary information when their personal data are processed in accordance with the Norwegian Public Limited Liability Companies Act (as outlined above); Mowi also needs to ensure that the company’s privacy policy intended to provide information on the collection of personal data from third parties is appropriately phrased and includes all of the information required under the GDPR.

Mowi has already indicated its intention to update its privacy policy, and transparency documentation and routines. In particular, after having received Datatilsynet’ advance notification, Mowi informed Datatilsynet of its intention to introduce the following changes to its privacy policy:

It shall include information on processing of the personal data of shareholders, collected via third parties such as Nasdaq.

It shall describe Mowi’s legal basis for processing shareholders personal data. The legal basis is GDPR article 6 (1) (f), on account of Mowi’s legitimate interest in knowing its investors, in order to follow-up investors and provide these with relevant information on the company. As a listed corporation, our investor relations department meet with a lot of investors throughout the year. A shareholder overview of relevant investors is therefore needed to maintain proper investor relations services.

The privacy policy shall describe that data processors may be recipients of the personal data processed, cf. the GDPR article 14 (1) (e).

International data transfers and suitable safeguards shall be described, cf. GDPR article 14 (1) (f), e.g. transfers to Nasdaq on the basis of Standard Contractual Clauses.

The information on retention periods in accordance with GDPR article 14 (2) (a) shall be supplemented.⁶⁷

Further, the company stated that “[a]ll updated information in the privacy policy will be updated correspondingly in Mowi’s internal documentation and routines.”⁶⁸

⁶⁶ Transparency Guidelines, page 38.

⁶⁷ See DPA’S ADVANCE NOTIFICATION – REPRIMAND AND COMPLIANCE ORDER – MOWI ASA (ref: 514012).

⁶⁸ Ibid.

Nonetheless, to make sure that these changes are actually and properly implemented, we deem it necessary to formally order Mowi to bring its information routines and documentation into compliance with Article 14 GDPR, and to notify the measures taken for complying with such order to Datatilsynet within four weeks after having received the present decision, in accordance with Article 58(2)(d) GDPR.

While the present inquiry has only focused on Mowi's compliance with Articles 12, 14 and 15 GDPR in connection with the above-mentioned complaint, this is without prejudice to the possibility of opening future inquiries to assess Mowi's compliance with Article 13 GDPR, including with respect to its privacy policy.

7. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.⁶⁹

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Senior Legal Advisor

This letter has electronic approval and is therefore not signed

⁶⁹ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

ZALARIS ASA
Postboks 1053 Hoff
0218 OSLO

Your reference

Our reference

21/02873-22

Date

10.05.2022

Compliance Order - Zalaris ASA

1. Introduction

The Norwegian Data Protection Authority (“Datatilsynet”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“GDPR”)¹ with respect to Norway.

On 18 March 2022, we notified Zalaris ASA (“Zalaris”, “you”, “your”, “the company”) of our intention to order Zalaris to comply in full with an access request it received on 28 September 2021 from a data subject residing in Germany. We also informed Zalaris that it could submit written representations in relation to the advance notification in question by 8 April 2022. However, Zalaris did not submit any written representations to Datatilsynet within the said deadline.

On 11 April 2022, Datatilsynet submitted a draft decision—which essentially reproduced the above advance notification—to the other supervisory authorities concerned in accordance with Article 60(3) GDPR. None of the other supervisory authorities concerned expressed a relevant and reasoned objection to the draft decision within four weeks after having been consulted by Datatilsynet.

Thus, the present decision is adopted in conformity with the advance notification we sent to Zalaris and the draft decision we submitted to the other supervisory authorities concerned.

2. Decision

Pursuant to Article 58(2)(d), we order Zalaris to:

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

Provide the complainant with all of the information he requested and is entitled to receive pursuant to Article 15 GDPR, including complete information on the purposes of the processing, the categories of personal data concerned, and the relevant storage period(s). Further, Zalaris shall provide the complainant with a copy of all of his personal data that are being processed by the company and have not yet been sent to him, unless Zalaris is able to demonstrate that one of the exceptions set out in Articles 12(5) and 15(4) GDPR or Article 16 of the Norwegian Personal Data Act applies. The information shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Zalaris shall notify the measures taken for complying with this decision to Datatilsynet within four weeks after having received the present decision.

Our inquiry has only focused on Zalaris' compliance with Articles 12 and 15 GDPR in connection with the above-mentioned complaint. Thus, the present decision is without prejudice to the possibility of opening future inquiries into Zalaris' compliance with other provisions of the GDPR, including with the broader transparency requirements imposed by Articles 5(1)(a) and 13 GDPR, as well as the data erasure requirements set out in Articles 5(1)(e) and 17.

3. Factual Background

On 14 July 2021, the complainant—i.e. a data subject residing in Germany who used to be employed in the German subsidiary of Zalaris (i.e., Zalaris Deutschland GmbH, which was merged with Zalaris Deutschland AG)—wrote to [REDACTED]—to exercise his right of access under Article 15 GDPR.² In particular, he requested the following information:

- [...] [sic] due to article 15 EU GDPR I would like to obtain following information from ZALARIS ASA:
- *Information about Automated Decision Logic if applicable*
 - *Information about the Right of correction and limitation*
 - *Information about the Right to complaint*
 - *The name and contact data of Controller*
 - *The name and contact data of Data protection officer*
 - *The Data Protection Guarantee if applicable*
 - *A complete copy of personal data in an easily visible, intelligible and clearly legible manner*
 - *The purposes of processing*
 - *The period of storage*
 - *The categories of personal data*
 - *The recipients of data transfer*
 - *The data source [...].*³

² See complaint dated 26 August 2021.

³ Ibid.

As he received no response from the company, on 26 August 2021, the data subject filed a complaint against Zalaris with Datatilsynet.⁴

After having received such a complaint, on 26 September 2021, Datatilsynet recommended the complainant to resubmit his access request by sending an email to gdpr@zalaris.com (i.e. the email address for submitting data protection inquiries provided in the privacy policy on Zalaris' website).⁵ Thus, on 28 September 2021, the complainant resubmitted his access request by forwarding the email he had sent to [REDACTED] to gdpr@zalaris.com.⁶ However, on 31 October 2021, the complainant informed Datatilsynet that, even after having sent this second email, he had not received any response from Zalaris.⁷

On 1 November 2021, Datatilsynet wrote to Zalaris to inquire about the aforementioned access requests.⁸ Datatilsynet's letter ordered Zalaris to respond to several questions on the case at hand by 30 November 2021. However, on 1 December 2021, Datatilsynet had still not received any answer from Zalaris. Thus, we sent a reminder to the company on the same date.⁹

Further to the above reminder, on 1 December 2021, Zalaris replied to Datatilsynet and claimed that the delay was due to the fact that the email with the response for Datatilsynet had remained in the outbox folder of the sender without him noticing it.¹⁰

As for the access request(s) at issue in the present case, in its reply to Datatilsynet, Zalaris stated that the company processed only the personal data that were relevant for the data subject's employment in Germany.¹¹ However, Zalaris' reply referred to a different email that [REDACTED] received from the complainant on 14 July 2021, which he (rightfully) did not interpret as an access request pursuant to Article 15 GDPR.¹²

After having received Zalaris' reply, on 1 December 2021, Datatilsynet wrote to Zalaris to stress that our inquiry concerned a different email, and once again asked the company to provide information on the access request that the complainant sent to [REDACTED] on 14 July 2021 at 17:23, and to gdpr@zalaris.com on 28 September 2021 at 13:29.¹³

On 2 December 2021, [REDACTED] wrote the following to Datatilsynet:

⁴ Ibid.

⁵ See Datatilsynet's email to the complainant dated 26 September 2021.

⁶ See complainant's email to Zalaris dated 28 September 2021.

⁷ See complainant's email to Datatilsynet dated 31 October 2021.

⁸ See Krav om redegjørelse - innsyn i personopplysninger (ref: 21/02873-9) dated 1 November 2021.

⁹ See Datatilsynet's email to Zalaris dated 1 December 2021 (sent at 15:56).

¹⁰ See Zalaris' email to Datatilsynet dated 1 December 2021 (stating: "Beklageligvis så gikk denne ikke ut umiddelbart den 8.11 da den ble skrevet da den ble lagende som draft i min utboks"). This appears to be evidenced by the fact that the letter with Zalaris' response that was eventually sent to Datatilsynet was dated 8 November 2021.

¹¹ See Zalaris' letter to Datatilsynet dated 8 November 2021 (but received by Datatilsynet on 1 December 2021) (stating: "Vi behandler kun personopplysninger relevant for hans ansattforhold og utbetaling av lønn.").

¹² Ibid. See too the email that the complainant sent to [REDACTED] on 14 July 2021 at 18:02 (annexed to Zalaris' reply to Datatilsynet).

¹³ See Datatilsynet's email to Zalaris dated 1 December 2021 (sent at 17:44).

[...] We have now investigated the case further.

It now turns out that I, as CEO of Zalaris, received an email on July 14 while I was on vacation. For information, Zalaris has approximately 880 employees in 14 countries and I receive at least 200+ emails daily. I have not had any direct relationship with the complainant as he was previously employed by our German subsidiary Zalaris Deutschland AG. The email was forwarded to the management in Germany on 16 July, where the former employee – [i.e., the complainant] – who demanded access had been employed until the end of September 2019.

Our German management responded to a similar request from [the complainant's] lawyer in April 2021, and a copy of the stored data was sent in electronic format to the lawyer as part of the conclusion of a settlement agreement. As the case was considered closed, the inquiry dated 14 July was therefore not answered further.

The inquiry to gdpr@zalaris.com seems to have been treated as spam due to the form and unknown email address in our systems. We have not received any other reminders or requests for access through another channel.

We from the Zalaris Group will now answer the relevant inquiry in the next few days and at the same time review the quality of our routines to ensure that similar future inquiries are answered in a timely manner [...] (our translation).¹⁴

On 22 December 2021, Zalaris replied to the data subject's access request as follows:

[...] We have received a notification by the Norwegian Data Protection authority that you have not received a response on the below article 15 request dated 14th of July and a similar request that shall have been sent to gdpr@zalaris.com on the 28th of September.

As your initial request was sent to my private email in the middle of my vacation, I forwarded this to our German management for action. As they were of the opinion that they had responded to a similar request by your lawyer in April 2021 where a copy of your data was requested, and they were of the opinion that they had settled outstanding issues with you, they did not proceed with a further response.

¹⁴ See Zalaris' email to Datatilsynet dated 2 December 2021 (stating in Norwegian: "Vi har nå undersøkt saken nærmere. Det viser seg nå at jeg som CEO for Zalaris har mottatt mail som referert til 14. juli mens jeg var på ferie. Til info så har Zalaris ca. 880 ansatte i 14 land og jeg mottar minst 200+ mail daglig. Jeg har ikke hatt noen direkte relasjon med klageren da denne tidligere var ansatt i vårt tyske datterselskap Zalaris Deutschland AG. Emailen ble den 16.7 videreført til ledelsen i Tyskland hvor den tidligere ansatte – [klageren] - som krevet innsyn hadde vært ansatt frem til slutten av september 2019. Vår tyske ledelse besvarte en tilsvarende henvendelse fra [klageren]'s advokat i April 2021 hvorpå kopi av lagrede data ble oversendt i elektronisk format til advokaten som et ledd i inngåelse av et forlik om sluttavtale. Da saken var ansett som avsluttet ble det derfor ikke henvendelsen datert 14. juli besvart ytterligere. Henvendelsen til gdpr@zalaris.com ser ut til å ha blitt oppfattet som søppelpost pga form og ukjent mail adresse i våre systemer. Vi har ikke fått andre påminnelser eller ønske om innsyn formidlet i annen kanal. Fra Zalaris Group vil vi nå besvare den aktuelle henvendelsen ila de nærmeste dagene og samtidig kvalitetssikre våre rutiner med mål at tilsvarende fremtidige saker blir besvart rettidig.").

The email sent to gdpr@zalaris.com appears to have been caught by our junk mail filter and has as such not been processed in due time in our systems. We are changing our solution for gdpr@zalaris.com to a forms based process on our web site with the goal of limiting the likelihood of similar incidents in the future.

Attached you will find a copy of our policy on GDPR article 15 responding to the items listed in your email. You will receive a copy of the data that we have about you in our systems via registered mail to your official address of residence. This will be delivered on print and on electronic format in the form of a password protected USB stick. Upon your response to the receipt of this email, we will forward you the password.

*We apologize for the inconvenience that the delay has caused as both adhering to GDPR requirements and responding to previous employees requests has the highest priority. [...]*¹⁵

On 26 January 2022, the complainant wrote to Datatilsynet that he had received a USB stick from Zalaris, but not the password to open the files contained in it.¹⁶ In response to a query from Datatilsynet, the complainant also claimed that he did not receive any email from Zalaris on 22 December 2021.¹⁷ Thereafter, Datatilsynet advised the complainant to contact Zalaris to ask the company to send such an email once again, as well as the password.¹⁸

On 28 January 2022, the complainant wrote to Zalaris and asked the company to resend the email Zalaris had sent to him on 22 December 2021, as well as the password to access the files in the USB stick he had received.¹⁹ On the same date, Zalaris forwarded the requested email to the complainant, and provided the relevant password.²⁰

On 2 March 2022, the complainant wrote to Datatilsynet that—in his view, after having examined Zalaris’ response—the company had not fully complied with his access request.²¹ On the same date, the complainant also wrote the following to Zalaris:

[...] [sic] After checking the USB stick, it shows that there is no password protection. All files are freely accessible.

I'm amazed that most of the data belongs to the ZALARIS Deutschland AG and ZALARIS Deutschland GmbH. I had requested the data that is processed at ZALARIS ASA.

¹⁵ See Zalaris’ email to the complainant dated 22 December 2021. The email also included Zalaris’ privacy policy (entitled “Regulation of Zalaris ASA’s processing of personal data”, and dated 21 December 2021) as an attachment (hereinafter “Regulation of Zalaris ASA’s processing of personal data”). Zalaris forwarded that email to Datatilsynet on the same date.

¹⁶ See complainant’s email to Datatilsynet dated 26 January 2022.

¹⁷ See complainant’s email to Datatilsynet dated 28 January 2022. This appears to be due to some technical issues on the complainant’s end, as Datatilsynet had received a copy of the email in question from Zalaris on 22 December 2022.

¹⁸ See Datatilsynet’s email to the complainant dated 28 January 2022.

¹⁹ See complainant’s email to Zalaris dated 28 January 2022.

²⁰ See Zalaris’ email to the complainant dated 28 January 2022.

²¹ See complainant’s email to Datatilsynet dated 2 March 2022.

I.e. the ZALARIS ASA has no data from me!

So this means:

- i) I received a letter from ZALARIS Deutschland attorney that there are no personal information from me! But you have it.*
- ii) You have no purpose and no confirmation to process personal data of me regarding ZALARIS Deutschland.*
- iii) There is no group privilege to use data from subsidiaries. You are not authorized to process incorrect or unauthorized data.*
- iv) The information about the ZALARIS ASA is wrong. You have at least my claim from 19.11.2021 and the personal data from the contract documents for the purchase/sale of ROC Ltd. But this is not part of your answer!*

Therefore I request the following:

- 1. Immediate deletion of all my personal data regarding ZALARIS Deutschland incl. all data transferred to third parties.*
- 2. Immediate payment of my claim from 19.11.2022*
- 3. Immediate payment of the second rate for the purchase/sale of ROC Ltd.*
- 4. Immediate information about my personal data processed at Zalaris ASA.*

Please inform me about the implementation within the next 2 weeks.

[...]

PS: Some notes regarding transparency.

The data sent does not correspond to the legal requirements (see Art. 15 GDPR):

missing: the purposes of the processing;

missing: the categories of personal data concerned;

missing: 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;

where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

missing: 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;

missing: the right to lodge a complaint with a supervisory authority;

where the personal data are not collected from the data subject, any available information as to their source;

missing: 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.

missing: 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.

Sometimes (for SAP data) there are some screenshots only, many dates (e.g. data from cluster tables) missing: The controller shall provide a copy of the personal data undergoing processing. 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.

Due to art. 12 GDPR the date must be “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”. There are many unknown data and data in English (e.g. for legal German topics) included.

Due to art. 20 GDPR and due to the court verdict I havn’t [sic] got all in a structured, commonly used and machine-readable format (e.g. screenshots). [...].²²

On 2 March 2022, Zalaris replied:

[...] Zalaris ASA has no other data related to your employment with us other than the data that you have received.

We are of the opinion that our response to you included all elements that you claim are missing.

In addition, we as Zalaris ASA signed contractual agreements with you as a commercial party and seller of shares in ROC Ltd, before you became an employee through ROC Deutschland

GmbH. This is commercial documentation archived in our contract archive with you as the seller and Zalaris as the buyer. We do not consider this material in the context of GDPR related to your employment with Zalaris. [...].²³

On 18 March 2022, Datatilsynet notified Zalaris of our intention to order the company to comply in full with the access request it received on 28 September 2021 from the complainant.²⁴

²² See complainant’s email to Zalaris dated 2 March 2022.

²³ See Zalaris’ email to the complainant dated 2 March 2022.

²⁴ See Varsel om pålegg - Zalaris ASA (ref: 21/02873-15). A copy of the advance notification was also sent to the complainant on the same date.

We also informed Zalaris that it could submit written representations in relation to the advance notification in question by 8 April 2022.²⁵ However, Zalaris did not submit any written representations to Datatilsynet within the said deadline.

4. Legal Background

4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

[...] applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Moreover, Article 3(1) GDPR provides that the Regulation:

[...] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

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

Pursuant to Article 4(2) GDPR:

“processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pursuant to Article 4(7) GDPR:

²⁵ Ibid., section 7.

“controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Pursuant to Article 4(9) GDPR:

“recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

4.3. The Right of Access by the Data Subject

Article 15 GDPR reads:

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 in such processing, the significance and envisaged consequences of such processing for the data subject;*

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.*

Furthermore, Article 12(1) to (4) GDPR provides 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.*

4.4. Competence, Tasks and Powers of Supervisory Authorities under the GDPR

Pursuant to Article 55(1) GDPR:

Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Further, Article 56(1) reads as follows:

Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

The term “main establishment” is defined in Article 4(16) GDPR as follows:

“main establishment” means:

(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 of personal data 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; [...].

The term “cross-border processing” is defined in Article 4(23) as follows:

“cross-border processing” means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Pursuant to Article 58(2) GDPR:

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

(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

- (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;
- (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;
- (e) to order the controller to communicate a personal data breach to the data subject;
- (f) to impose a temporary or definitive limitation including a ban on processing;
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
- (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;
- (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.

4.5. EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area (“EEA”) Agreement by means of Decision of the EEA Joint Committee No 154/2018 (“EEA Joint Committee Decision”).²⁶

Article 1(b) of the EEA Joint Committee Decision provides that:

[...] the terms “Member State(s)” and “supervisory authorities” shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.

²⁶ Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.²⁷ The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet's Competence

Zalaris is a multinational company offering human resources and payroll administration services. It has its headquarter in Norway, but has operations and offices in several European countries, including in Sweden, Denmark, Finland, Germany, France, Ireland, Latvia, Lithuania, Estonia and Poland.

Thus, Zalaris has several establishments in the EU/EEA, including in Norway, and in the context of the activities of these establishments it processes personal data, including personal data of the employees of its group. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of the complainant, Zalaris qualifies as a controller (within the meaning of Article 4(7) GDPR), as Zalaris itself acknowledges.²⁸

As Zalaris has a main establishment (within the meaning of Article 4(16) GDPR) in the EEA and its processing of the complainant's personal data is cross-border (within the meaning of Article 4(23) GDPR), the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that Zalaris' main establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR.

6. Datatilsynet's Assessment

6.1. Zalaris' Failure to Respond to the Complainant's Access Request in a Timely Manner

Under Article 12(3) GDPR, controllers are required to respond to access requests submitted pursuant to Article 15 GDPR "without undue delay and in any event within one month of receipt of the request." However, in exceptional circumstances, that period may be extended by two further months.

²⁷ Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").

²⁸ See Regulation of Zalaris ASA's processing of personal data (stating: "Data Controller. The responsible for the processing of personal data that we carry out about you is Zalaris ASA, represented by Managing Director, [REDACTED] and Data protection officer, [REDACTED].").

In the present case, Zalaris itself acknowledged that it failed to respond to the complainant's access requests within the above deadline.²⁹ However, Zalaris claimed that this was due to the fact that the first request was sent directly to the CEO of the company, while the second ended up in the spam folder of the company's email inbox.³⁰

As for the request sent directly to [REDACTED] on 14 July 2021, our view is that not much can be reproached to Zalaris. As noted by the European Data Protection Board (EDPB):

The controller is [...] not obliged to act on a request sent to the e-mail address of a controller's employee who may not be involved in the processing of requests concerning data subjects' rights [...]. Such requests shall not be considered effective, if the controller has clearly provided the data subject with appropriate communication channel.³¹

Hence, given that the privacy policy available on Zalaris' website at the time did provide a specific email address to be used for data protection inquiries (i.e., gdpr@zalaris.com),³² it was legitimate to expect data subjects (including the complainant) to submit access requests through such a communication channel, and not directly to the CEO of the Zalaris. Indeed, the CEO of a company of the size of Zalaris cannot be expected to be directly involved in the processing of requests concerning data subjects' rights. Therefore, in our view, Zalaris did not violate Articles 12(2) and 15 GDPR by failing to respond to the email that the complainant sent directly to [REDACTED] [REDACTED] on 14 July 2021. In this regard, it should be noted that—contrary to what was argued by the complainant³³—where personal data are processed by a company (which decides on the means and purposes of the processing) it is the company as such that qualifies as the “controller”, and not its CEO.³⁴

However, under Article 12(2) GDPR, controllers have an obligation to “facilitate the exercise” of the data subject right under Article 15 GDPR. This entails—among other things—that controllers should take adequate technical and organizational measures to ensure that they can receive and handle in a timely manner the access requests they receive from data subjects. In the words of the EDPB:

The controller should provide appropriate and user-friendly communication channels that can easily be used by the data subject.³⁵

²⁹ See Zalaris email to Datatilsynet dated 2 December 2021.

³⁰ Ibid.

³¹ EDPB, Guidelines 01/2022 on data subject rights - Right of access (Version 1.0, Adopted on 18 January) (hereinafter “EDPB Guidelines on the Right of Access”), para. 55.

³² See: <<https://web.archive.org/web/20201123184817/https://zalaris.com/privacy/privacy-policy/#>>. All web links provided in this letter were last accessed on 3 March 2022.

³³ See complainant’s email to Datatilsynet dated 28 September 2021 (stating: “due to Art.15 ‘the data subject shall have the right to obtain from the controller’. That’s what I had done! [REDACTED] is the controller and have to answer. So he broke the law!”).

³⁴ Kuner et al., *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020), p. 149.

³⁵ EDPB Guidelines on the Right of Access, p. 2.

This means that, although controllers remain free to decide which specific communication channel should be used for submitting access requests, they must ensure that the communication channel they implement is easy to use and effective. Thus, if a controller decides to receive access requests via email, it must make sure that the email account it uses for this purpose implements state-of-the-art anti-spam protection—which does not treat legitimate access requests as spam—and/or that it monitors the spam folder on a regular basis to identify the presence of possible legitimate access requests. Effective anti-spam solutions (e.g., CAPTCHA solutions) do exist and should be adequately considered by the controller, in accordance with its accountability obligations under the GDPR.³⁶

In the present case, Zalaris' anti-spam solution failed to “facilitate” the exercise of the right under Article 15 GDPR, in breach of Article 12(2) GDPR, as it treated a legitimate access request as spam, leading to such a request remaining unanswered for almost 3 months.

Nonetheless, we consider such an infringement to be minor,³⁷ for the following reasons:

- It appears to have affected a single data subject, as—to date—Datatilsynet has not received any other complaints concerning Zalaris' compliance with Articles 12(2) and 15 GDPR;
- After Datatilsynet's inquiry, Zalaris discontinued the use of the email address which treated the complainant's access request as spam, and embedded a new communication channel with a CAPTCHA solution in its privacy policy to be used for sending data protection inquiries;³⁸ and
- Although Zalaris did not respond to the complainant's access request submitted on 28 September 2021 within the standard statutory one month period—as it should have done under Article 12(3) GDPR—the company did respond on 22 December 2021 within the maximum 3 months period envisaged by Article 12(3) GDPR.

In light of the above, Datatilsynet considers that—in the present case—it is not warranted to issue any corrective measures for this infringement, and considers this specific matter to be settled.

6.2. Zalaris' Failure to Provide All of the Information Required under Article 15 GDPR

Under Article 15(1) (a) to (h) and 15(2) GDPR, data subjects are entitled to obtain from the controller specific information regarding the processing of their personal data. In his access request, the complainant required Zalaris to provide him with essentially all of the information that he is entitled to obtain under Article 15(1) (a) to (h) and 15(2) GDPR. Indeed, he requested:

³⁶ Arts. 5(2) and 24 GDPR.

³⁷ Cf. rec. 148 GDPR.

³⁸ See: <<https://zalaris.com/privacy/privacy-policy/>>.

- *Information about Automated Decision Logic if applicable*
- *Information about the Right of correction and limitation*
- *Information about the Right to complaint*
- *The name and contact data of Controller*
- *The name and contact data of Data protection officer*
- *The Data Protection Guarantee if applicable*
- *A complete copy of personal data in an easily visible, intelligible and clearly legible manner*
- *The purposes of processing*
- *The period of storage*
- *The categories of personal data*
- *The recipients of data transfer*
- *The data source [...].³⁹*

Zalaris responded to such a request essentially by sending a copy of—at least some of—the personal data of the complainant that are being processed by the company, and a copy of the company’s privacy policy applicable to employees’ data.⁴⁰

While Zalaris’ privacy policy does provide some of the information requested by the complainant, it does not appear to be always sufficiently granular to allow the complainant to understand and assess all of the processing operations actually carried out with regard to his personal data. As noted by the EDPB:

In order to comply with Art. 15(1)(a) to (h) and 15(2), controllers may carefully use text modules of their privacy notice as long as they make sure that they are of adequate actuality and preciseness with regards to the request of the data subject. Before or at the beginning of the data processing, some information, such as the identification of specific recipients or the specific duration of the data processing, will often only be possible in general terms. Furthermore, privacy notices as well as records of processing activities generally relate to processing concerning all data subjects and are often not tailored to the situation of a specific data subject. Some information, like for example the right to complain to a supervisory authority (see Art. 15(1)(f)), does not change depending on the person making the access request. Therefore, it may be communicated in general terms as it is also done in the privacy notice. Other types of information, such as the information on recipients, on categories and on the source of the data may vary depending on who makes the request and what the scope of the request is. In the context of an access request under Art. 15, any information on the processing available to the controller may therefore have to be updated and tailored for the processing operations actually carried out with regard to the data subject making the request. Thus, referring to the wording of its privacy policy would not be a sufficient way for the controller to give information required by Art. 15(1)(a) to (h) and (2) unless the «tailored» information is the same as the «general» information.⁴¹

³⁹ See complainant’s email to Zalaris dated 28 September 2021.

⁴⁰ Ibid.

⁴¹ EDPB Guidelines on the Right of Access, para. 111.

In our view, by simply sending a copy of its privacy policy to the complainant, Zalaris has not provided sufficient information about the following:

- Purposes of the processing (Article 15(1)(a)). Zalaris' privacy policy simply states: "The purpose of Zalaris ASA's processing of personal data is primarily ensuring that we take care of you as an employee and the fulfillment of the obligations we have undertaken to implement the contract with you. We will also process personal data to the extent that the law imposes or gives us access to such processing or when you have consented to such processing. In addition to this, personal data is processed for the following purposes: [...] Answer any incoming inquiries."⁴² However, it would appear that Zalaris processes the personal data of the complainant also for other purposes (e.g. establishment, exercise or defence of legal claims against the complaint; performance of a settlement agreement with the complainant, etc.) which are not mentioned in the privacy policy. As noted by the EDPB, "Information on the purposes according to Art. 15(1)(a) needs to be specific as to the precise purpose(s) in the actual case of the requesting data subject. It would not be enough to list the general purposes of the controller without clarifying which purpose(s) the controller pursues in the current case of the requesting data subject."⁴³
- Categories of personal data concerned (Article 15(1)(b)). Zalaris' privacy policy does not provide information on what kinds of personal data are being processed other than by stating that "Name, phone number, email address and any personal information that may result from the inquiry."⁴⁴ As noted by the EDPB, "Information on categories of data (Art. 15(1)(b)) [...] may also have to be tailored to the data subject's situation. [...]. If a request of access is made on the basis of Art. 15 GDPR, the data subject who makes the request must, in addition to the access to the actual data being processed (component 2), in line with Art. 15(1)(b) also be informed as to the specific categories of data which are being processed in the specific case (e.g. only e-mail address, but not the telephone number)."⁴⁵
- Storage period(s) (Article 15(1)(d)). Zalaris' privacy policy merely states: "We will delete or anonymize personal data about you when the purpose of the specific processing is fulfilled, unless the personal data is or may be kept beyond this as a consequence of a legal requirement. This means, for example, that personal data we process on the basis of your consent will be deleted if you withdraw your consent. Personal information we process to fulfill an agreement with you will be deleted when the agreement is fulfilled and all obligations arising from the agreement are fulfilled. Zalaris has established archiving and deletion rules."⁴⁶ This information does not enable the data subject to assess, on the basis of his own situation, what the retention period will be for specific data/purposes. Indeed, as noted by the EDPB, "The information given by the controller has to be precise enough for the data subject to know how long

⁴² See Regulation of Zalaris ASA's processing of personal data.

⁴³ EDPB Guidelines on the Right of Access, para. 112.

⁴⁴ See Regulation of Zalaris ASA's processing of personal data.

⁴⁵ EDPB Guidelines on the Right of Access, para. 113.

⁴⁶ See Regulation of Zalaris ASA's processing of personal data.

the data relating to the data subject will continue to be stored. If it is not possible to specify the time of deletion, the duration of storage periods and the beginning of this period or the triggering event (e.g. termination of a contract, expiration of a warranty period, etc.) shall be specified.”⁴⁷ This is particularly relevant in this case, given that the employment contract with the complainant has already been terminated.

In contrast, contrary to what has been claimed by the complainant,⁴⁸ the privacy policy seems to provide sufficient information on recipients (Article 15(1)(c)),⁴⁹ the existence of the right to rectification, erasure, restriction of processing and to object to such processing (Article 15(1)(e)),⁵⁰ the right to lodge a complaint with a supervisory authority (Article 15(1)(f)),⁵¹ the source of the personal data (Article 15(1)(g)),⁵² automated decision-making (Article 15(1)(h)),⁵³ and international transfers (Article 15(2)).⁵⁴

Further, it appears that Zalaris has not provided the complainant with a copy of *all* of his personal data that are being processed by the company. For instance, Zalaris denied to grant access to the complainant’s personal data contained in documents regarding the purchase/sale of ROC Ltd on the basis of the following:

Zalaris ASA signed contractual agreements with you as a commercial party and seller of shares in ROC Ltd, before you became an employee through ROC Deutschland

⁴⁷ EDPB Guidelines on the Right of Access, para. 116.

⁴⁸ See complainant’s email to Zalaris dated 2 March 2022.

⁴⁹ Zalaris’ privacy policy specifies that “Zalaris ASA uses the following data processors: Telecomputing (IT Supplier), Cut-e (Assessment tests), Meditor (Background checks), Netigate (invitations to events, internal temperature index survey)” (See Regulation of Zalaris ASA’s processing of personal data). We assume that these are the only relevant recipients. If that is not the case, Zalaris should also provide the complainant with complete information about recipients.

⁵⁰ Zalaris’ privacy policy states: “you may require access, correction or deletion of the personal information we process about you. You also have the right to demand us to limit the processing, to object to the processing, and request data portability”. See Regulation of Zalaris ASA’s processing of personal data.

⁵¹ Zalaris’ privacy policy states: “The Data Protection Authority’s task is to check that the privacy policy is being followed. Any complaints about Zalaris ASA’s processing of personal data that concerns you may be directed to your local Data Protection Authority or directly to the Norwegian Data Protection Authority.” See Regulation of Zalaris ASA’s processing of personal data.

⁵² Under Article 15(1)(g) GDPR, information on the source of personal data must be provided only insofar as they are “available” and “where the personal data are not collected from the data subject”. We understand that this is not applicable in this case. However, if Zalaris processed personal data that it has not collected from the complainant, it should provide him with any available information as to their source.

⁵³ Under Article 15(1)(h) GDPR, information on automated decision-making must be provided only insofar as it “exists”. This does not seem to be applicable in this case, as it does not seem that Zalaris engages in any automated decision-making with respect to the complainant.

⁵⁴ Zalaris’ privacy policy states: “We transfer personal data to countries outside the EU/EEA area in the following situations: According to DPA and internal agreements employee data management related to new hire, changes, terminations, payroll, travel etc. for Zalaris employees are handled by the HR team in India. The legal basis for such transfer is the Zalaris DPA” (See Regulation of Zalaris ASA’s processing of personal data). Based on this, we understand that Zalaris does not transfer the complainant’s personal data outside the EU/EEA, as the complainant is no longer an employee of Zalaris in Germany. Thus, Article 15(2) does not seem to be applicable in this case, as that provision only applies “where personal data are transferred to a third country”. However, if Zalaris transfers the personal data of the complainant outside the EU/EEA, the company should provide the complainant with the information required under Article 15(2) GDPR.

GmbH. This is commercial documentation archived in our contract archive with you as the seller and Zalaris as the buyer. We do not consider this material in the context of GDPR related to your employment with Zalaris. [...]. (emphasis added).⁵⁵

In this regard, we note that the fact that the personal data that Zalaris processes are *not* related to the employment relationship with the complainant is not *per se* sufficient to deny access to such data. As noted by the EDPB:

*If no limits or restrictions apply, data subjects are entitled to have access to all data processed relating to them, or to parts of the data, depending on the scope of the request [...] The obligation to provide access to the data does not depend on the type or source of those data. It applies to its full extent even in cases where the requesting person had initially provided the controller with the data, because its aim is to let the data subject know about the actual processing of those data by the controller.*⁵⁶

Thus, Zalaris must provide the complainant with a copy of *all* of his personal data that are being processed by the company, unless Zalaris is able to demonstrate that one of the exceptions set out in Articles 12(5) and 15(4) GDPR or Article 16 of the Norwegian Personal Data Act applies to such data.

However, this does not mean that Zalaris must necessarily provide a copy of the entire documents in which such personal data are contained. In this regard, the EDPB noted:

*[...] access to the data under Art. 15(1) comprises complete information on all data and cannot be understood as granting only a summary of the data. At the same time, the obligation to provide a copy is not designed to widen the scope of the right of access: it refers (only) to a copy of the personal data undergoing processing, not necessarily to a reproduction of the original documents [...].*⁵⁷

It further opined:

*[...] the GDPR expressly contains an obligation to provide the data subject with a copy of the personal data undergoing processing. This, however, does not mean that the data subject always has the right to obtain a copy of the documents containing the personal data, but an unaltered copy of the personal data being processed in these documents. Such copy of the personal data could be provided through a compilation containing all personal data covered by the right of access as long as the compilation makes it possible for the data subject to be made aware and verify the lawfulness of the processing.*⁵⁸

Therefore, we deem it necessary to order Zalaris, pursuant to Article 58(2)(d) GDPR, to provide the complainant with all of the information he requested and is entitled to receive pursuant to Article 15 GDPR. In particular, Zalaris shall provide the complainant with complete

⁵⁵ See Zalaris' email to the complainant dated 2 March 2022.

⁵⁶ EDPB Guidelines on the Right of Access, para. 19.

⁵⁷ Ibid., para. 23.

⁵⁸ Ibid., para. 150.

information on the following: (1) purposes of the processing; (2) categories of personal data concerned; and (3) relevant storage period(s). Further, Zalaris must provide the complainant with a copy of *all* of his personal data that are being processed by the company and have not yet been sent to the complainant, unless Zalaris is able to demonstrate that one of the exceptions set of in Articles 12(5) and 15(4) GDPR or Article 16 of the Norwegian Personal Data Act applies to such data.

The information and data provided to the complainant shall be understandable and clear to the complainant (see Article 12(1) GDPR). This entails—among other things—that Zalaris might need to supply the complainant with additional information that explains the data provided, if such data are not immediately intelligible. In this regard, the EDPB noted:

The requirement that the information is “intelligible” means that it should be understood by the intended audience, whilst keeping in mind any special needs that the data subject might have that is known to the controller. Since the right of access often enables the exercise of other data subject rights, it is crucial that the information provided is made understandable and clear. This is because data subjects will only be able to consider whether to invoke their right to, for example, rectification under Art. 16 once they know what personal data are being processed, for what purposes etc. As a result, the controller might need to supply the data subject with additional information that explains the data provided. It should be emphasised that the complexity of data processing puts an obligation on the controller to provide the means to make the data understandable and could not be used as an argument to limit the access to all data. Similarly, the obligation on the controller to provide data in a concise manner cannot be used as an argument to limit access to all data.⁵⁹

For completeness purposes, it should be noted that—contrary to what was argued by the complainant⁶⁰—Zalaris may provide the relevant information in English, as the complainant’s access request was written in English, and the complainant has been corresponding with Zalaris in English, which shows that he is sufficiently familiar with the English language. Further—also contrary to what was argued by the complainant⁶¹—the information does not need to be provided in a machine-readable format. In this regard, the EDPB opined:

It should be noted that the provisions on format requirements are different regarding the right of access and the right of data portability. Whilst the right of data portability under Art. 20 GDPR requires that the information is provided in a machine readable format, the right to information under Art. 15 does not. Hence, formats that are considered not to be appropriate when complying with a data portability request, for example pdf-files, could still be suitable when complying with a request of access.⁶²

While the present inquiry has only focused on Zalaris’ compliance with Articles 12 and 15 GDPR in connection with the above-mentioned complaint, this is without prejudice to the

⁵⁹ Ibid., para. 139.

⁶⁰ See complainant’s email to Zalaris dated 2 March 2022.

⁶¹ Ibid.

⁶² EDPB Guidelines on the Right of Access, para. 154.

possibility of opening future inquiries to assess Zalaris' compliance with its broader obligations under the GDPR, including with the transparency requirements imposed by Articles 5(1)(a) and 13 GDPR as well as the data deletion requirements laid down in Articles 5(1)(e) and 17.

7. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.⁶³

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Senior Legal Advisor

This letter has electronic approval and is therefore not signed

⁶³ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

Your reference

Our reference

21/01315-7

Date

19.08.2022

Rejection of Complaint - Wordfeud.aasmul.net

1. Introduction

The Norwegian Data Protection Authority (hereinafter “Datatilsynet”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“GDPR”)¹ with respect to Norway.

Between 25 September 2020 and 23 April 2021, Datatilsynet received several complaints regarding the website wordfeud.aasmul.net (hereinafter the “Website”), which led us to open three parallel inquiries (Cases No. 20/03786, 21/01315 and 21/01611).

All complaints came from purported users of the Website who had been allegedly banned from the Website for failing to provide a valid proof of identity, after having received an identity check request from a moderator of the Website.

While the complaints came from three different email addresses and were signed with different names, during the investigation Datatilsynet became wary of the fact that all complaints might actually come from a single individual. Thus, Datatilsynet asked all of the purported complainants to confirm whether they wished to maintain their complaint, and if so, to provide a postal address and telephone number that Datatilsynet could use to communicate with them, in line with our standard practice.² Only one complainant responded to Datatilsynet confirming that they wished to maintain their complaint. However, the complainant at hand failed to comply with Datatilsynet’s request regarding the contact details, as they provided us with a false postal address and a telephone number that is not in use, as outlined below.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

² See: <https://www.datatilsynet.no/en/about-us/contact-us/how-to-complain-to-the-norwegian-dpa/>

In light of the above deceitful behaviour and the need to be able to confirm the identity of the complainants to handle the matter submitted to Datatilsynet, we have decided to refuse to act on the complaints at hand.

2. Decision

Datatilsynet adopts the following decision:

- The complaint in Case No. 21/01315 shall be rejected pursuant to Article 57(4) GDPR due to its abusive and excessive character.
- Cases No. 20/03786 and 21/01611 are hereby closed, as the purported complainants in these cases failed to respond to Datatilsynet’s request to provide their contact details and confirm that they wished to maintain their complaint.

An advance notification of the present decision to the complainants has been omitted pursuant to Article 16(3)(b) and (c) of the Norwegian Public Administration Act.³

3. Factual Background

Between 25 September 2020 and 23 April 2021, Datatilsynet received three separate complaints regarding the website wordfeud.aasmul.net (hereinafter the “Website”) purportedly from three different individuals who claimed that they had been banned from that Website because they failed to provide a valid proof of identity.⁴ The individuals in question claimed that such an identity verification was in violation of the GDPR, and one of these individuals also claimed that the Website’s administrator failed to comply with an access and erasure request that they submitted pursuant to Articles 15 and 17 GDPR.⁵

The Website appears to be owned and run on a not-for-profit basis by Mr. Eskil Åsmul through a sole proprietorship: AASMUL.NET ESKIL ÅSMUL (hereinafter “AASMUL”). The Website organizes tournaments of Wordfeud and other digital board games. These tournaments are organized in different languages, including Danish, English, Finnish, French, German, Norwegian, Spanish and Swedish. Participation in the tournaments is free of charge, but participants may gain access to “extra statistics and training material” if they make a donation to the Website of at least 90 NOK, \$15, €12 or £10.⁶

To participate in the tournaments organized by the Website, an individual user must: (1) create a user name; (2) provide an email address; and (3) select the language in which they want to play.⁷ However, a player may voluntarily choose to provide additional information, including

³ Act of 10 February 1967 relating to procedure in cases concerning the public administration (“Forvaltningsloven”).

⁴ See emails to Datatilsynet dated 25 September 2020, 19 March 2021, and 23 April 2021.

⁵ See email to Datatilsynet dated 19 March 2021.

⁶ See <<https://wordfeud.aasmul.net/About.aspx>>.

⁷ See <<https://wordfeud.aasmul.net/Users.aspx>>.

home country, date of birth, real life name, profile picture, and link to a personal website.⁸ However, players may use a pseudonym to participate in the tournaments organized by the Website, and the email address and the other information they provide are as a rule not verified by the website.⁹

The Website makes use of a number of volunteers who act as moderators and are responsible for making sure that the tournaments on the Website run smoothly and that players comply with the relevant rules of the game they play.¹⁰ In some cases, moderators may decide to expel a player who violate such rules.¹¹

On 21 June 2021, Datatilsynet sent a letter to Mr. Åsmul asking him to provide his views on the issues raised by the complainants, and we received his response on 20 July 2021.¹²

In his letter to Datatilsynet, Mr. Åsmul explained that the Website does not carry out systematic identity checks on players. However, one of the Website's moderators suspected that a player who had been banned from the Website in the past due to misbehavior (e.g., cheating to improve their scores) was trying to regain access to the website under different fake identities. Thus, on an ad hoc basis, he asked some players who behaved suspiciously to prove their identity, in an attempt to prevent that the banned player would regain access to the Website.

This happened for instance with a player who claimed to be an American Professor named [REDACTED] (i.e., the same name of the complainant in Case No. 21/01315) who was playing exceptionally well on the version in French of Word feud, which was the version of the game that the above-mentioned banned player normally used. The player who claimed to be named [REDACTED] was asked to prove their identity by the moderator of the Website, and in response they provided a copy of an old library card, which the moderator considered to be an insufficient proof of identity, as it could have been easily forged. As the player refused to provide any other proof of identity, they were excluded from the game.

Mr. Åsmul further explained that, after the exclusion of the player in question, Mr. Åsmul received an access and erasure request from someone who claimed to be [REDACTED], but he did not comply with such a request as he had doubts concerning the identity of the person making the request.

In his response to Datatilsynet, Mr. Åsmul also cast doubts as to whether the complainant who claims to be [REDACTED] and the other two complainants in Cases 20/03786 and 21/01611 are in fact the same person.

In light of the above, and given that all complaints had been submitted to Datatilsynet via email (without providing any additional contact details), on 12 April 2022, Datatilsynet wrote to all three purported complainants the following message:

⁸ Ibid.

⁹ See AASMUL's letter to Datatilsynet of 20 July 2021.

¹⁰ See <<https://wordfeud.aasmul.net/About.aspx>>.

¹¹ See AASMUL's letter to Datatilsynet of 20 July 2021.

¹² Ibid.

“[...] If you still wish that we handle your complaint, please respond to the present email and provide us with your full name, postal address and a phone number where we can reach you.

Please note that if you will not respond to this email and provide the above information by 26 April 2022, we will deem that you no longer wish that we handle your complaint and we will therefore close your case.”¹³

On 12 April 2022, the complainant who claims to be named [REDACTED] replied that they wished that their complaint be handled by Datatilsynet adding: “You can reach me via e-mail at [REDACTED]”.¹⁴

Given the circumstances, on 12 April 2022, Datatilsynet replied that to handle the case we needed a postal address and a telephone number within the said deadline. Otherwise, Datatilsynet would record the information provided as a tip, which may be used for future investigative purposes.¹⁵

On 17 April 2022, the complainant responded as follows:

“[...] Name:

Dr. [REDACTED]

Postal Address:

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

Phone Number:

[REDACTED]

E-mail Address:

[REDACTED]

Please keep correspondence to e-mail. I do not wish to be contacted via post or phone.”

The other purported complainants did not respond to Datatilsynet within the above-mentioned deadline.

¹³ See email to the complainants dated 12 April 2022.

¹⁴ See email to Datatilsynet dated 12 April 2022.

¹⁵ See email to the complainant dated 12 April 2022.

4. Legal Background

4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

[...] applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Moreover, Article 3(1) GDPR provides that the Regulation:

[...] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

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

Pursuant to Article 4(2) GDPR:

“processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Pursuant to Article 4(7) GDPR:

“controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

4.3. Rights of the Data Subject

Article 15 GDPR reads:

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.*

Pursuant to Article 17 GDPR:

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 the personal data, the controller, taking account of available technology and the cost of 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 links to, or copy or replication of, those personal data.*

3. *Paragraphs 1 and 2 shall not apply to the extent 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) as well as Article 9(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.

Furthermore, Article 12(2) and (6) GDPR provides that:

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.

[...]

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.

In addition, Article 77 GDPR reads:

1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

2. The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

4.4. Competence and Tasks of Supervisory Authorities under the GDPR

Pursuant to Article 55(1) GDPR:

Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

Further, Article 56(1) reads as follows:

Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

The term “cross-border processing” is defined in Article 4(23) as follows:

“*cross-border processing*” means either:

- (a) *processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or*
- (b) *processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.*

Pursuant to Article 57(1)(f) GDPR:

Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

[...]

- (f) *handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary.*

Further, Article 57(4) GDPR provides:

Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs, or refuse to act on the request. The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

4.5. EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area (“EEA”) Agreement by means of Decision of the EEA Joint Committee No 154/2018 (“EEA Joint Committee Decision”).¹⁶

Article 1(b) of the EEA Joint Committee Decision provides that:

¹⁶ Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

[...] the terms “Member State(s)” and “supervisory authorities” shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.¹⁷ The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet’s Competence

The Website is run by Mr. Eskil Åsmul through a sole proprietorship in Norway, which constitutes the single establishment of the controller. However, the games on the Website are targeted at players in different EU/EEA countries, as the tournaments are organized in different languages, including Danish, English, Finnish, French, German, Norwegian, Spanish and Swedish. Thus, the processing of players’ personal data takes place in the context of the activities of a single establishment in the EU/EEA, but it is likely to substantially affect data subjects in several EU/EEA countries. Therefore, it qualifies as cross-border processing under Article 4(23)(b) GDPR.

In light of the above, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that the single establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. Therefore, a draft of the present decision was shared with the other supervisory authorities concerned, which did not raise any objections within a period of four weeks after having been consulted in accordance with Article 60(3) GDPR.

6. Datatilsynet’s Assessment

Datatilsynet’s view is that the demeanour assumed by the complainant in Case No. 21/01315 qualifies as an “abuse of rights”, which entails that their request is manifestly excessive. Consequently, the complaint should be rejected as “manifestly excessive” pursuant to Article 57(4) GDPR.

The prohibition of abuse of rights is a general principle of EU and EEA law.¹⁸ A determination of abuse of rights under EU/EEA law is based on a cumulative test combining objective and subjective elements. The objective element requires that it be evident from the specific set of circumstances in question that, despite formal observance of the conditions laid down by the EU/EEA rules, the purpose of those rules has not been achieved. The subjective element

¹⁷ Act No 38 of 15 June 2018 relating to the processing of personal data (“personopplysningsloven”).

¹⁸ CJEU, Case C-321/05, *Kofoed v Skatteministeriet*, para. 38; EFTA Court, Case E-1/20, *Kerim v The Norwegian Government*, para. 36.

requires an abusive intention to obtain an advantage from the EU/EEA rules by artificially creating the conditions laid down for obtaining it.¹⁹

The prohibition applies also with respect to the rights laid down in the GDPR, including the right to lodge a complaint set out in Article 77 GDPR, as other supervisory authorities have previously noted.²⁰ Therefore, the scope of the right set out in Article 77 GDPR cannot be extended to cover abusive practices that are conducted for the purpose of deceitfully obtaining advantages that ordinarily could have resulted from a lawful use of such a right (e.g., obtaining that a supervisory authority orders the controller to stop a certain processing operation, such as identity verification).

Whilst identification of the complainant is not invariably a condition for the exercise of the right laid down in Article 77 GDPR, the effective exercise of the powers that supervisory authorities enjoy under the GDPR may require that the competent authority be able to confirm the identity the complainant, in particular in cases that concern alleged infringements of data subject rights.

Of relevance in this regard is the following statement by the EFTA Court in Joined Cases E-11/19 and E-12/19, *Adpublisher*:

“the effective functioning of data protection compliance under the GDPR may require disclosing the complainant’s personal data to the data controller. This would be the case, *inter alia*, when the data subject, in accordance with point (c) of Article 58(2) of the GDPR, requests to exercise his or her rights or alleges infringement of his or her rights by the controller. Acting on this request, *a supervisory authority may need to disclose the identity of a complainant to the controller* to enable the latter to fulfil the order. In turn, *the supervisory authority’s exercise of its powers*, in accordance with, *inter alia*, points (e) to (g) and (j) of Article 58(2) of the GDPR, *may necessitate disclosing the identity of the complainants to the controller.*”²¹ (emphasis added)

Furthermore, Article 12(2) and (6) GDPR – which a supervisory authority must take into account when assessing whether a controller has legitimately refused to act upon a data subject’s request – provides that:

“[...] 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.*

[...]

¹⁹ EFTA Court, Case E-1/20, *Kerim v The Norwegian Government*, para. 37; CJEU, Case C-202/13, *The Queen, on the application of Sean Ambrose McCarthy and Others v Secretary of State for the Home Department*, para. 54.

²⁰ See Spanish Supervisory Authority (AEPD), Procedimiento N°: E/00739/2021.

²¹ EFTA Court, Joined Cases E-11/19 and E-12/19, *Adpublisher*, para. 51.

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.*” (emphasis added)²²

Moreover, if a supervisory authority has reasonable doubts concerning the complainant’s identity, but nonetheless issues orders related to such an identity without eliminating these doubts, it may run the risk of applying the law incorrectly or causing harm to other data subjects should the identity at hand prove to be false.

Thus, in some cases, such as the present one, supervisory authorities need to be able to confirm the identity of the complainant.

This is reflected in the guidance on “How to Complain to the Norwegian Data Protection Authority” available on Datatilsynet’s website, which indicates that a complaint should include, among other things, “contact information (name, phone and postal address only)”.²³ Providing contact information is not an invariable condition for lodging a complaint with Datatilsynet. Additionally, Datatilsynet accepts anonymous tips, although these are generally taken into account only for planning possible future investigative activities.²⁴ However, as set out above, in some cases we need to be able to confirm the identity of the complainant to handle the relevant complaint with all due diligence.

In Case No. 21/01315, the complainant claims, among other things, that the controller failed to act on their request for exercising their rights under Articles 15 and 17 GDPR. At the same time, in the context of our investigation, Mr. Åsmul raised concerns that the purported complainant is engaging in fraudulent behaviour, operating under a false identity (or identities) to try to be readmitted to the Website following their exclusion, and that they may be trying to manipulate Datatilsynet accordingly in their quest.

Further, Mr. Åsmul’s specific doubts with regard to the identity of the complainants, as well as a closer scrutiny of the different complaints, made Datatilsynet wary of the fact that all such complaints might have been submitted by a single individual under multiple pretended identities. In this respect, it should be noted that the complaints present very similar features and linguistic patterns. For example, they all came from Gmail accounts; they all used the term “GDPR violations” in the subject line; they all complained about a Norwegian company called “Wordfeud League of Honour”, which does not exist; they all used the term “raise a complaint”, which is rather unusual and not in line with standard data protection terminology;²⁵ they all used the term “data privacy policy”, which is not a standard term under the GDPR; and none of the complaints provided any contact details other than an email address, despite the fact that on Datatilsynet’s website it is clearly indicated (also in English) that a complaint should include “name, phone and postal address”.

²² See further Recital 64 GDPR, which states: “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 [...].”

²³ See: <https://www.datatilsynet.no/en/about-us/contact-us/how-to-complain-to-the-norwegian-dpa/>

²⁴ See: <https://www.datatilsynet.no/om-datatilsynet/kontakt-oss/tips-oss/>

²⁵ The common terminology is “submit” or “lodge” a complaint.

Under this specific set of circumstances, Datatilsynet deemed it necessary to confirm the identity of the complainants to handle their complaints, also in light of its duty to handle complaints with all due diligence.²⁶ Hence, on 12 April 2022, it sent the following message to all of the purported complainants:

“[...] If you still wish that we handle your complaint, please respond to the present email and provide us with your full name, postal address and a phone number where we can reach you.

Please note that if you will not respond to this email and provide the above information by 26 April 2022, we will deem that you no longer wish that we handle your complaint and we will therefore close your case [...].”²⁷

Only the complainant in Case No. 21/01315 replied to the above message within the said deadline. However, they first insisted to be contacted via email and did not provide any other contact information.²⁸ Only upon our further insistence, they provided us with the following contact information on 21 April 2022:

“Name:

[REDACTED]

Postal Address:

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

Phone Number:

[REDACTED]

E-mail Address:

[REDACTED]

Please keep correspondence to e-mail. I do not wish to be contacted via post or phone.”²⁹

²⁶ CJEU, Case C-311/18, *Facebook Ireland and Schrems*, para. 109.

²⁷ See emails to the complainants dated 12 April 2022.

²⁸ See email from the complainant dated 12 April 2022.

²⁹ See email from the complainant dated 21 April 2022.

Upon receiving such information, Datatilsynet realized that the address provided by the complainant corresponded to the address of an UPS store in West York (USA),³⁰ which offers mailbox services.³¹ Datatilsynet contacted the store in question to confirm whether a person named [REDACTED] rented a mailbox at that store, possibly mailbox "#341". The store manager responded that no one named "[REDACTED]" rented a mailbox at their store, and there was no mailbox with a number as high as 341 at the store. Thereafter, Datatilsynet tried to call the phone number provided by the complainant, which turned out to be not in use. Therefore, it became apparent that Datatilsynet had been provided with false information, presumably to lure us into taking action against AASMUL, which would facilitate the complainant's readmission to the Website.

In light of the above, in our view, the complainant in Case No. 21/01315 committed an abuse of the right set out in Article 77 GDPR. This is because they acted in bad faith by providing Datatilsynet with false personal information, and tried to deceitfully obtaining advantages that could have ordinarily resulted from a lawful use of such a right. Moreover, the fact that none of the other complainants replied to Datatilsynet and the identified similarities among the various complaints received by Datatilsynet suggest that the same person attempted to lure Datatilsynet into believing that several different individuals experienced similar data protection issues with the Website. Further, the person in question appears to have done all this not so much to uphold their data protection rights, but to seek Datatilsynet's support in bypassing their exclusion from the Website, which is not the purpose of the complaint mechanism set out in the GDPR. Thus, the complainant's behaviour qualifies as an "abuse of rights" under EU/EEA law.

The abusive character of the request of the complainant is indirectly confirmed by the fact that several recitals of the GDPR make clear that identity frauds and other forms of frauds should be limited and prevented.³²

An abusive request is "manifestly excessive" for the purposes of Article 57(4) GDPR, as it goes manifestly beyond the purposes for which the complaint mechanism set out in the GDPR was envisaged.³³ This is further confirmed by the EFTA Court's finding in *Campbell* that the scope of EEA law—which includes the GDPR and its complaint mechanism—cannot be extended to cover abuses.³⁴ In this respect, it should be noted that the words "in particular" in Article 57(4) indicate that a request may be considered "excessive" not only when it is "repetitive".

Thus, Datatilsynet has decided to refuse to act on the complaint in Case No. 21/01315 in accordance with Article 57(4) GDPR. Datatilsynet has also decided to close Cases 20/03786 and 21/01611, as the purported complainants in these cases failed to respond to Datatilsynet's request to provide their contact details (hence making their identification impossible) and confirm that they wished to maintain their complaints.

³⁰ See: <https://locations.theupsstore.com/pa/york/2159-white-st>

³¹ See: <https://locations.theupsstore.com/pa/york/2159-white-st/mailbox-services>

³² See e.g., Rec. 47, 75, 85 and 88.

³³ The purpose of the right to lodge a complaint is to ensure adequate protection of the rights of the data subject. See Rec. 141 GDPR.

³⁴ EFTA Court, Case E-4/19, *Campbell*, para. 69.

However, this is without prejudice to the possibility of opening future inquiries into AASMUL's compliance with the GDPR, including with respect to sporadic identity checks.

7. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.³⁵

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Senior Legal Advisor

This letter has electronic approval and is therefore not signed

Recipient(s):
[REDACTED]

Copy to: AASMUL.NET ESKIL ÅSMUL

³⁵ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

[REDACTED]
[REDACTED]
[REDACTED] OSLO

Exempt from public disclosure:

*Offl. § 13, jf. personopplysningsloven § 24 første ledd 2.
punktum*

Your reference

Our reference

20/01759-12

Date

04.10.2022

Final Decision - Raise Gruppen AS og Raise Norway AS

IMI article 56 entry number:	57051
IMI case register:	62626
National case reference:	NO SA: 20/01759 & 18/02429
Controller:	Raise Gruppen AS and Raise Norway AS
Date of complaint:	29 August 2018

We refer to the abovementioned cross-border case where Datatilsynet (the Norwegian Data Protection Authority, hereinafter "NO SA") has been identified as the lead supervisory authority pursuant to Article 56(1) GDPR¹. Integritetsskyddsmyndigheten (the Swedish Data Protection Authority) has been identified as the sole supervisory authority concerned pursuant to Article 4(22) GDPR.

The NO SA adopts the following decision:

The NO SA rejects the complaint submitted against Nikita Hair on 29 August 2018 (Case 18/02429 & 20/01759).

Factual Background

On 29 August 2018, the NO SA received a complaint (the "**Complaint**") against the chain of hairdressers trading under the names Nikita Hair and Hairshop. The background of the Complaint was that in connection with drop-in hairdresser appointments (i.e. where the complainant tried to get a haircut by simply turning up at the salon) at both Hairshop and Nikita Hair branches in Oslo on 27 August and 28 August 2018 respectively, the complainant had to provide both their full name and telephone number (the "**Requested Personal Data**") before they could get a haircut.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1.

When the complainant asked an employee at Hairshop what the purpose of requiring the Requested Personal Data was, the employee answered that it was needed in case the complainant complained about the service. When the complainant asked the same question to an employee of Nikita Hair, the employee answered that the information was needed in case of a financial audit. In both cases, the complainant would have paid by way of a bank card.

In the Complaint, the complainant specified that their complaint related to whether:

- Nikita Hair had a real need for, and reasonable grounds to require the provision of, the Requested Personal Data; and
- whether the Requested Personal Data was only used in connection with financial audits, particularly as the complainant had received a text message from Nikita Hair requesting feedback.

On 17 November 2021, the NO SA sent an order to provide information to Raise Gruppen AS, who was specified as Nikita Hair's contact point for information regarding processing of personal data. The NO SA requested Raise Gruppen AS who the controller for the processing is, and if they were the controller to explain how personal data relating to drop-in hairdresser appointments are processed in accordance with the Norwegian Data Protection Act and the GDPR.

On 17 December 2021, Raise Gruppen AS responded to the NO SA's order to provide information dated 17 November 2021. Raise Gruppen AS explained their group company structure, and that its previous wholly owned subsidiaries Nikita Hair Norway AS (trading as Nikita Hair) and Sayso Hair & Style AS (trading as Sayso, previously Hairshop) had now been merged into one wholly owned subsidiary called Raise Norway AS. In addition, the same is true for the wholly owned Swedish subsidiaries Nikita Hair Sweden AB (trading as Nikita Hair) and Sayso Hair & Style AB (trading as Sayso, previously Hairshop) which merged into one wholly owned subsidiary called Raise Sweden AB.

Raise Gruppen AS also confirmed that the booking system for all customers is handled centrally by the administration in Raise Gruppen AS, and that Raise Gruppen AS is therefore largely the controller of processing activities connected to this system. In connection with the restructuring of the group, Raise Gruppen AS stated they were currently reviewing their privacy policy including to make it clear what the processing relationship between the group companies and customer rights is.

Raise Gruppen AS stated that in the case of the complained of processing operation, and in relation to the Requested Personal Data, the legal basis for processing is to fulfil the legal obligations that follow from the requirements of the Norwegian Bookkeeping Act (Nw. Bokføringsloven) and the Norwegian Bookkeeping Regulations (Nw. Bokføringsforskriften). Section 5-15 of the Norwegian Bookkeeping Regulations stipulates what documentation businesses that provide services by appointment must keep, and specified that the time of when the service was carried out, the customer name and as far as possible the name of the person carrying out the service shall be documented. The same provision also specified that it applies to appointments that are not made beforehand (i.e. drop-in appointments). Raise Gruppen AS stated that when implementing a new booking system, they wanted to be able to offer

anonymous drop-in appointments, but they obtained an external legal assessment on the obligations under the Norwegian Bookkeeping Regulations which confirmed that they were not able to offer anonymous drop-in appointments. In addition, the external legal assessment stated that they needed to register "contact details" for drop-in customers in order to fulfil a legal obligation pursuant to Article 6(2) GDPR, Section 5-15 of the Norwegian Bookkeeping Regulations and the Norwegian Bookkeeping Act. Raise Gruppen AS also stated that they were of the understanding that the same rules applied in Sweden.

On 26 January 2022, the NO SA sent a further order to provide information to Raise Gruppen AS ordering them to explain for what purpose, and under which legal basis, they processed the telephone numbers of drop-in customers in Norway, and for what purpose and under which legal basis they processed the name and telephone numbers of drop-in customers in Sweden.

On 21 February 2022, Raise Gruppen AS responded to the NO SA's order to provide information dated 26 January 2022. Raise Gruppen AS explained that, due to their understanding of the intention behind the Norwegian Bookkeeping Act and consequently the Norwegian Bookkeeping Regulations, to prevent a black market and money-laundering through securing auditability of transactions covered by the law, it is necessary to be able to distinguish individual customers in the booking system. Raise Gruppen AS therefore used telephone numbers as an identifier to secure compliance with the Norwegian Bookkeeping Act. The legal basis for processing the name of drop-in customers is therefore Article 6(1)(c) GDPR, and the legal basis for processing the telephone number of drop-in customers is Article 6(1)(f) GDPR as a practical way to implement the requirement to be able to distinguish between customers. The same applies for drop-in customers in Sweden, albeit instead in relation to the Swedish Bookkeeping Act (1999:1078).

Legal Background

Pursuant to Article 6(1) GDPR, as adapted pursuant to Annex XI of the EEA Agreement as amended by the Decision of the EEA Joint Committee No 154/2018 of 6 July 2018:

- 1. 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.

2. Member States [and EFTA States] may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
 - a. [the EEA Agreement]; or
 - b. Member State [and EFTA State] law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The [EEA Agreement, Member State or EFTA State] law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Findings

The Complaint focuses on why Nikita Hair requires both a drop-in customer's name and telephone number prior to offering a haircut. Therefore the focus of the NO SA's assessment will be on the matter of the legal basis for processing the name and telephone number of drop-in customers at Nikita Hair, as the NO SA deems that this would constitute investigating the complaint to the extent appropriate.

The legal basis allegedly relied upon when processing the name of drop-in customers is Article 6(1)(c) GDPR in order to comply with the Norwegian Bookkeeping Act and Norwegian

Bookkeeping Regulations. The Norwegian Bookkeeping Regulations imposes a duty on those carrying out services by appointment, including by drop-in appointments, to collect and process the name of the customer. The NO SA notes that only the entity under the obligation of the legal obligation may rely on Article 6(1)(c), as such legal obligation would mandate the purpose and means of the processing on the entity under such obligation. As such, the controller for such processing operation must be Raise Norway AS (following the merger of Nikita Hair Norway AS and Sayso Hair & Style Norway AS into one company and renaming such company Raise Norway AS), as that is the entity that carried out the service for the complainant and therefore the entity to which the obligations of the Norwegian Bookkeeping Regulations apply. The NO SA therefore finds that the processing of drop-in customer names can validly be based on Article 6(1)(c) GDPR, but notes that Raise Gruppen AS appears to have misunderstood to which legal entity such legal basis relates and therefore which legal entity is the controller.

The legal basis relied upon when processing the telephone numbers of drop-in customers is Article 6(1)(f) GDPR as a practical way to implement the intention behind the Norwegian Bookkeeping Act and Norwegian Bookkeeping Regulations by distinguishing between customers. The NO SA considers that this interest is a legitimate one, and it is unlikely that such interest is overridden by the interests or fundamental rights and freedoms of the data subject when having regard to the purpose of the processing.

In relation to the processing of the complainant's telephone number for the purpose of sending a text message to the complainant requesting feedback after their haircut, the NO SA notes that Raise Gruppen AS has stated they are normally the controller in relation to processing activities connected to the booking system (i.e. they have determinative influence in deciding the purposes and means of processing). The NO SA further notes that Raise Gruppen AS did not specifically elaborate on the legal basis relied upon for this processing activity. However, the NO SA considers it is unlikely Raise Gruppen AS did not have a legal basis for this specific processing activity, particularly as a customer relationship had been established at the time the processing activity was carried out (i.e. after the complainant had received a haircut). The NO SA deems that it would be disproportionate to investigate this part of the complaint any further.

Based on the above, the NO SA deems this case to be investigated to the extent appropriate and did not identify any infringement of Article 6 GDPR. The NO SA therefore rejects the Complaint, and considers the case closed.

The NO SA nonetheless considers that both Raise Norway AS and Raise Gruppen AS would benefit from being reminded of their obligations under the GDPR. Therefore the NO SA will send a separate letter to them pointing out the same, particularly in relation to identifying who the controller is for a given processing activity, ensuring that transparent information is given to data subjects as to how and why their personal data is processed and a controller's responsibilities generally.

Right of appeal

As this decision has been adopted by the NO SA pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section

22 of the Norwegian Data Protection Act. This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
juridisk rådgiver

This letter has electronic approval and is therefore not signed

Copy to: Raise Gruppen AS and Raise Norway AS

[REDACTED]
[REDACTED]
[REDACTED] OSLO

Exempt from public disclosure:

*Offl. § 13, jf. personopplysningsloven § 24 første ledd 2.
punktum*

Your reference

Our reference

20/01759-12

Date

04.10.2022

Final Decision - Raise Gruppen AS og Raise Norway AS

IMI article 56 entry number:	57051
IMI case register:	62626
National case reference:	NO SA: 20/01759 & 18/02429
Controller:	Raise Gruppen AS and Raise Norway AS
Date of complaint:	29 August 2018

We refer to the abovementioned cross-border case where Datatilsynet (the Norwegian Data Protection Authority, hereinafter "NO SA") has been identified as the lead supervisory authority pursuant to Article 56(1) GDPR¹. Integritetsskyddsmyndigheten (the Swedish Data Protection Authority) has been identified as the sole supervisory authority concerned pursuant to Article 4(22) GDPR.

The NO SA adopts the following decision:

The NO SA rejects the complaint submitted against Nikita Hair on 29 August 2018 (Case 18/02429 & 20/01759).

Factual Background

On 29 August 2018, the NO SA received a complaint (the "**Complaint**") against the chain of hairdressers trading under the names Nikita Hair and Hairshop. The background of the Complaint was that in connection with drop-in hairdresser appointments (i.e. where the complainant tried to get a haircut by simply turning up at the salon) at both Hairshop and Nikita Hair branches in Oslo on 27 August and 28 August 2018 respectively, the complainant had to provide both their full name and telephone number (the "**Requested Personal Data**") before they could get a haircut.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1.

When the complainant asked an employee at Hairshop what the purpose of requiring the Requested Personal Data was, the employee answered that it was needed in case the complainant complained about the service. When the complainant asked the same question to an employee of Nikita Hair, the employee answered that the information was needed in case of a financial audit. In both cases, the complainant would have paid by way of a bank card.

In the Complaint, the complainant specified that their complaint related to whether:

- Nikita Hair had a real need for, and reasonable grounds to require the provision of, the Requested Personal Data; and
- whether the Requested Personal Data was only used in connection with financial audits, particularly as the complainant had received a text message from Nikita Hair requesting feedback.

On 17 November 2021, the NO SA sent an order to provide information to Raise Gruppen AS, who was specified as Nikita Hair's contact point for information regarding processing of personal data. The NO SA requested Raise Gruppen AS who the controller for the processing is, and if they were the controller to explain how personal data relating to drop-in hairdresser appointments are processed in accordance with the Norwegian Data Protection Act and the GDPR.

On 17 December 2021, Raise Gruppen AS responded to the NO SA's order to provide information dated 17 November 2021. Raise Gruppen AS explained their group company structure, and that its previous wholly owned subsidiaries Nikita Hair Norway AS (trading as Nikita Hair) and Sayso Hair & Style AS (trading as Sayso, previously Hairshop) had now been merged into one wholly owned subsidiary called Raise Norway AS. In addition, the same is true for the wholly owned Swedish subsidiaries Nikita Hair Sweden AB (trading as Nikita Hair) and Sayso Hair & Style AB (trading as Sayso, previously Hairshop) which merged into one wholly owned subsidiary called Raise Sweden AB.

Raise Gruppen AS also confirmed that the booking system for all customers is handled centrally by the administration in Raise Gruppen AS, and that Raise Gruppen AS is therefore largely the controller of processing activities connected to this system. In connection with the restructuring of the group, Raise Gruppen AS stated they were currently reviewing their privacy policy including to make it clear what the processing relationship between the group companies and customer rights is.

Raise Gruppen AS stated that in the case of the complained of processing operation, and in relation to the Requested Personal Data, the legal basis for processing is to fulfil the legal obligations that follow from the requirements of the Norwegian Bookkeeping Act (Nw. Bokføringsloven) and the Norwegian Bookkeeping Regulations (Nw. Bokføringsforskriften). Section 5-15 of the Norwegian Bookkeeping Regulations stipulates what documentation businesses that provide services by appointment must keep, and specified that the time of when the service was carried out, the customer name and as far as possible the name of the person carrying out the service shall be documented. The same provision also specified that it applies to appointments that are not made beforehand (i.e. drop-in appointments). Raise Gruppen AS stated that when implementing a new booking system, they wanted to be able to offer

anonymous drop-in appointments, but they obtained an external legal assessment on the obligations under the Norwegian Bookkeeping Regulations which confirmed that they were not able to offer anonymous drop-in appointments. In addition, the external legal assessment stated that they needed to register "contact details" for drop-in customers in order to fulfil a legal obligation pursuant to Article 6(2) GDPR, Section 5-15 of the Norwegian Bookkeeping Regulations and the Norwegian Bookkeeping Act. Raise Gruppen AS also stated that they were of the understanding that the same rules applied in Sweden.

On 26 January 2022, the NO SA sent a further order to provide information to Raise Gruppen AS ordering them to explain for what purpose, and under which legal basis, they processed the telephone numbers of drop-in customers in Norway, and for what purpose and under which legal basis they processed the name and telephone numbers of drop-in customers in Sweden.

On 21 February 2022, Raise Gruppen AS responded to the NO SA's order to provide information dated 26 January 2022. Raise Gruppen AS explained that, due to their understanding of the intention behind the Norwegian Bookkeeping Act and consequently the Norwegian Bookkeeping Regulations, to prevent a black market and money-laundering through securing auditability of transactions covered by the law, it is necessary to be able to distinguish individual customers in the booking system. Raise Gruppen AS therefore used telephone numbers as an identifier to secure compliance with the Norwegian Bookkeeping Act. The legal basis for processing the name of drop-in customers is therefore Article 6(1)(c) GDPR, and the legal basis for processing the telephone number of drop-in customers is Article 6(1)(f) GDPR as a practical way to implement the requirement to be able to distinguish between customers. The same applies for drop-in customers in Sweden, albeit instead in relation to the Swedish Bookkeeping Act (1999:1078).

Legal Background

Pursuant to Article 6(1) GDPR, as adapted pursuant to Annex XI of the EEA Agreement as amended by the Decision of the EEA Joint Committee No 154/2018 of 6 July 2018:

- 1. 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.

2. Member States [and EFTA States] may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
 - a. [the EEA Agreement]; or
 - b. Member State [and EFTA State] law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The [EEA Agreement, Member State or EFTA State] law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Findings

The Complaint focuses on why Nikita Hair requires both a drop-in customer's name and telephone number prior to offering a haircut. Therefore the focus of the NO SA's assessment will be on the matter of the legal basis for processing the name and telephone number of drop-in customers at Nikita Hair, as the NO SA deems that this would constitute investigating the complaint to the extent appropriate.

The legal basis allegedly relied upon when processing the name of drop-in customers is Article 6(1)(c) GDPR in order to comply with the Norwegian Bookkeeping Act and Norwegian

Bookkeeping Regulations. The Norwegian Bookkeeping Regulations imposes a duty on those carrying out services by appointment, including by drop-in appointments, to collect and process the name of the customer. The NO SA notes that only the entity under the obligation of the legal obligation may rely on Article 6(1)(c), as such legal obligation would mandate the purpose and means of the processing on the entity under such obligation. As such, the controller for such processing operation must be Raise Norway AS (following the merger of Nikita Hair Norway AS and Sayso Hair & Style Norway AS into one company and renaming such company Raise Norway AS), as that is the entity that carried out the service for the complainant and therefore the entity to which the obligations of the Norwegian Bookkeeping Regulations apply. The NO SA therefore finds that the processing of drop-in customer names can validly be based on Article 6(1)(c) GDPR, but notes that Raise Gruppen AS appears to have misunderstood to which legal entity such legal basis relates and therefore which legal entity is the controller.

The legal basis relied upon when processing the telephone numbers of drop-in customers is Article 6(1)(f) GDPR as a practical way to implement the intention behind the Norwegian Bookkeeping Act and Norwegian Bookkeeping Regulations by distinguishing between customers. The NO SA considers that this interest is a legitimate one, and it is unlikely that such interest is overridden by the interests or fundamental rights and freedoms of the data subject when having regard to the purpose of the processing.

In relation to the processing of the complainant's telephone number for the purpose of sending a text message to the complainant requesting feedback after their haircut, the NO SA notes that Raise Gruppen AS has stated they are normally the controller in relation to processing activities connected to the booking system (i.e. they have determinative influence in deciding the purposes and means of processing). The NO SA further notes that Raise Gruppen AS did not specifically elaborate on the legal basis relied upon for this processing activity. However, the NO SA considers it is unlikely Raise Gruppen AS did not have a legal basis for this specific processing activity, particularly as a customer relationship had been established at the time the processing activity was carried out (i.e. after the complainant had received a haircut). The NO SA deems that it would be disproportionate to investigate this part of the complaint any further.

Based on the above, the NO SA deems this case to be investigated to the extent appropriate and did not identify any infringement of Article 6 GDPR. The NO SA therefore rejects the Complaint, and considers the case closed.

The NO SA nonetheless considers that both Raise Norway AS and Raise Gruppen AS would benefit from being reminded of their obligations under the GDPR. Therefore the NO SA will send a separate letter to them pointing out the same, particularly in relation to identifying who the controller is for a given processing activity, ensuring that transparent information is given to data subjects as to how and why their personal data is processed and a controller's responsibilities generally.

Right of appeal

As this decision has been adopted by the NO SA pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section

22 of the Norwegian Data Protection Act. This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

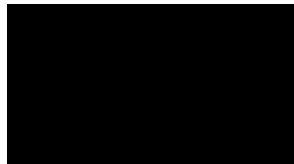
Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
juridisk rådgiver

This letter has electronic approval and is therefore not signed

Copy to: Raise Gruppen AS and Raise Norway AS



Exempt from public disclosure:

*Offl. § 13, jf. Personopplysningsloven § 24 første led 2.
punktum*

Your reference

Our reference

20/01693-16

Date

11.11.2022

Final Decision - Equinor ASA

IMI article 56 entry number:	363967
IMI case register:	427314
National case reference:	NO SA: 20/01693 & 19/03512
Controller:	Equinor ASA
Date of complaint:	14 November 2019

We refer to the abovementioned cross-border case where Datatilsynet (the Norwegian Data Protection Authority, hereinafter "NO SA") has been identified as the lead supervisory authority pursuant to Article 56(1) GDPR¹. The data protection authorities in the following countries have indicated that they are supervisory authorities concerned pursuant to Article 4(22) GDPR: Belgium, Denmark, France, Germany and the Netherlands.

The NO SA adopts the following decision:

The NO SA rejects the complaint submitted against Equinor ASA (Case 20/01693 & 19/03512).

Factual Background

Complaint

On 14 November 2019, the NO SA received a complaint against Equinor ASA ("Equinor"). The complainant alleged:

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119/1.

- Equinor had not complied with the complainants request to have their personal data deleted in time, as Equinor deleted the personal data 38 days after having received the complainant's request for deletion;
- Equinor outsource their recruitment process to the British company Alexander Mann Solutions and job seekers do not have control over their data and do not know what is saved on Alexander Mann Solutions' servers, where, how long, how it is processed, how it is used etc.

On 26 January 2020, the NO SA received further correspondence from the complainant with further information in relation to their complaint against Equinor. The complainant further alleged:

- Equinor uses the job seeker platform "www.peopleclick.eu", and the websites of Alexander Mann Solutions and www.peopleclick.eu are unsecure as they use http and not https.

On 13 April 2022, the NO SA received further correspondence from the complainant with updated information, the salient points of which were:

- Jobseekers using peopleclick cannot update or delete their information (applications, CV, e-mail address), nor can jobseekers delete their account;
- Equinor's privacy policy does not give jobseekers open and satisfactory information about the recruitment process, recruitment platform, recruitment partners etc. that are used by Equinor.

Investigation by the NO SA

From the documentation received from the complainant, the NO SA considers that the complaint covers the following issues:

- Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12 GDPR)
- Information to be provided where personal data are collected from the data subject (Article 13 GDPR)
- The right to erasure (Article 17 GDPR)
- Security of processing (Article 32 GDPR) in relation to the encryption of data in transit regarding Equinor's recruitment management system

The NO SA notes from the documentation provided by the complainant that the complainant had sent an e-mail to Equinor on 11 June 2019 requesting deletion of their profile. Equinor responded to the complainant on 10 July 2019 confirming that their profile had been deleted. The NO SA cannot find a breach of Articles 12(3) or 16 GDPR in this regard, as Equinor responded to the complainant and deleted the complainant's personal data within 1 month from the complainant's request. The NO SA did not take any further action with regard to the complainant's allegations in relation to the deletion request.

On 6 April 2022, the NO SA sent Equinor an order to provide information requesting them, in relation to the period between around summer 2019 and January 2020 (the relevant period) and currently to:

- Describe and explain Equinor's use of Alexander Mann Solutions and the platform «www.peopleclick.eu» in Equinor's recruitment process, including
 - The relationship between Peopleclick, AMS and Equinor
 - Which processing activities AMS carries out on behalf of Equinor, and how Peopleclick is used in this regard
 - How you have taken into consideration the security of processing in relation to the relevant processing activities pursuant to Article 32
 - Whether and how you have ensured that job applicants are provided with information about the relevant processing activities pursuant to Articles 12, 13 and if applicable 14, including in relation to the relevant processing activities.

On 19 May 2022, Equinor responded to the NO SA's order to provide information dated 6 April 2022. The salient points from such response are detailed below:

- Equinor use both Alexander Mann Solutions AS ("AMS") and Peoplefluent Ltd ("PeopleFluent") as data processors in their general external and internal recruitment process. Equinor further provided the NO SA with copies of their data processing agreements with both AMS and PeopleFluent.
- Equinor has since 2012 utilised a recruitment management system delivered as a software as a service solution by PeopleFluent (the "RMS"). The personal data for the recruitment processes are stored and processed in the RMS.
- AMS has since 2014 been Equinor's main supplier of recruitment assistance. Only authorised personnel from AMS have role-based access to the RMS to carry out their tasks, meaning they have access to the RMS and all data stored in the system. Access to the RMS is controlled by Equinor, and the access is removed when any resources from AMS leave the Equinor account. AMS does not process personal data in their own systems on behalf of Equinor, but rather have access to the RMS.
- Equinor states that the RMS is and was during the relevant time period encrypted. PeopleFluent use encryption protocols for data at rest and in back-up, as well as transport layer security (TLS) for data in transfer. Equinor provided the NO SA with PeopleFluent's security documentation overview as well as extracts of audits of the RMS between 1 October 2018 and 31 October 2020 in relation to this matter showing that no exceptions were noted in relation to encryption in transit or at rest.
- Equinor uses a layered approach to informing data subjects about the processing of personal data it carries out, depending on the purposes for the processing and whether or not the data subject is an internal or external applicant. Equinor provided the NO SA with copies of privacy policies in force in the relevant period and currently, as well as explained with screenshots how such privacy policies are displayed to users.
- Job candidates applying for positions with Equinor can view their personal data and application status in the PeopleFluent system by logging in to their profile. Personal

data is automatically deleted after 12 months, but candidates can request to have their data deleted sooner by contacting Equinor through Equinor's contact form.

Legal Background

Pursuant to Article 12(1), (2) and (3) GDPR:

Transparent information, communication and modalities for the exercise of the rights of the data subject

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.*

...

Pursuant to Article 13 GDPR, as adapted pursuant to Annex XI of the EEA Agreement as amended by the Decision of the EEA Joint Committee No 154/2018 of 6 July 2018:

Information to be provided where personal data are collected from the data subject

1. *Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
 - a. *the identity and the contact details of the controller and, where applicable, of the 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 basis for the processing;
 - d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
 - e. the recipients or categories of recipients of the personal data, if any;
 - 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 [applicable pursuant to the EEA Agreement], 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.
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
- a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
 - c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - d. the right to lodge a complaint with a supervisory authority;
 - e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
 - f. 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.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Pursuant to Article 17 (1)(a) and (b) GDPR:

Right to erasure ('right to be forgotten')

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;*

...

Pursuant to Article 32(1) and (2) GDPR:

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.*
- ...

Findings

The complainant alleged that Equinor had not complied with their request to have their personal data deleted in time as Equinor deleted the personal data 38 days after having received the complainant's request for deletion. In addition, the complainant alleged that jobseekers using "peopleclick" cannot update or delete their information (applications, CV, e-mail address), nor

can jobseekers delete their account. The NO SA has interpreted this allegation as being related to Equinor's RMS. Based on the documentation provided by the complainant themselves, it appears that the time between the complainant requesting deletion of their personal data and Equinor responding to the complainant confirming that their personal data had been deleted was less than one month. The NO SA also notes that Equinor's privacy policies, in force both in the relevant period and currently, tell data subjects that they may update or delete their personal data as well as how they may contact Equinor, as controller, to exercise these rights. The NO SA cannot see that Equinor has breached Articles 12, 13 or 17 GDPR, and therefore rejects these parts of the complaint.

The complainant alleged that Equinor outsource their recruitment process to the British company Alexander Mann Solutions and job seekers do not have control over their data and do not know what is saved on Alexander Mann Solutions' servers, where, how long, how it is processed, how it is used etc. In addition, the complainant alleged Equinor's privacy policy does not give jobseekers open and satisfactory information about the recruitment process, recruitment platform, recruitment partners etc. that are used by Equinor. Based on the documentation provided by Equinor, PeopleFluent and AMS are processors of Equinor. PeopleFluent is specifically mentioned in Equinor's recruitment privacy policy in force both in the relevant period and currently, and AMS would fall under the category of "external recruitment / employment verification service providers contracted by the Equinor Group" mentioned in such privacy policy. The NO SA notes Equinor's general or recruitment-specific privacy policies, in force in the relevant period and currently, mention amongst other things what personal data are stored and where, for how long, and why and how it is processed and used - which the complainant specifically stated were missing. In addition, the NO SA has been provided with screenshots showing that the privacy policy specific to recruitment is accessible prior to creating an account in Equinor's RMS, and one must confirm that this privacy policy has been read before creating an account. The NO SA therefore rejects these parts of the complaint.

The complainant alleged that Equinor uses the job seeker platform "www.peopleclick.eu", and the websites of Alexander Mann Solutions and www.peopleclick.eu are unsecure as they use http and not https. Equinor provided the NO SA with PeopleFluent's security documentation overview as well as extracts of audits of the RMS between 1 October 2018 and 31 October 2020 in relation to this matter showing that no exceptions were noted in relation to encryption in transit or at rest. As such, the NO SA cannot find any substantiation to this matter raised by the complainant, and Equinor has provided the NO SA with evidence to the contrary of such allegation. The NO SA therefore rejects this part of the complaint.

In light of the above, the NO SA considers that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR. The NO SA has not been able to identify a breach of the GDPR based on such investigation, and the complaint as a whole is therefore rejected.

Right of appeal

As this decision has been adopted by the NO SA pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section

22 of the Norwegian Data Protection Act. This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Legal Adviser

This letter has electronic approval and is therefore not signed

Copy to: Equinor ASA

SATS ASA
Postboks 4949 NYDALEN
0423 OSLO

Your reference

Our reference

20/02422-9

Date

06.02.2023

Administrative Fine - SATS ASA

1. Introduction and Summary

The Norwegian Data Protection Authority (hereinafter “Datatilsynet”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“GDPR”)¹ with respect to Norway.

Between 2 October 2018 and 8 December 2021, Datatilsynet received several complaints against SATS ASA (hereinafter “SATS”, “you”, “your”, “the company”). In essence, all such complaints concerned alleged infringements of data subjects’ rights committed by SATS, in particular in connection with its handling of data subjects’ requests submitted pursuant to Articles 15 and 17 GDPR.

After having investigated all of these complaints, Datatilsynet hereby issues an administrative fine of NOK 10 000 000 (ten million) against SATS for having violated Articles 5(1)(a) and (e), 6(1), 12, 13, 15 and 17 GDPR.

2. Datatilsynet’s Decision

Pursuant to Article 58(2)(i) GDPR, Datatilsynet issues an administrative fine of NOK 10 000 000 (ten million) against SATS ASA for:

- having infringed Articles 12(3) and 15 GDPR by failing to timely act upon two separate access requests;
- having infringed Articles 5(1)(e), 12(3) and 17 GDPR by failing to take prompt action and erase certain personal data without undue delay pursuant to three separate erasure requests;

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

- having infringed Articles 5(1)(a), 12(1) and 13 GDPR by failing to duly inform data subjects about its data retention policy concerning the personal data of banned members, and the relevant legal basis for the processing; and
- having infringed Articles 5(1)(a) and 6(1) GDPR by failing to rely on a valid lawful basis to process the training history data of the members of its fitness centers.

Our inquiry has only focused on SATS' compliance with Articles 5, 6, 12, 13, 15 and 17 GDPR in connection with the complaints against SATS lodged with Datatilsynet between 2 October 2018 and 8 December 2021. Thus, the present decision is without prejudice to the possibility of opening future inquiries into SATS' compliance with other provisions of the GDPR and with respect to other data subjects.

3. Factual Background

On 2 October 2018, Datatilsynet received a complaint against SATS (Case 20/01746, previously 18/03153).² This complaint was submitted by a member of the fitness centers run by SATS in Norway (hereinafter “Complainant No 1”) who essentially claimed that in May 2018 (or earlier), SATS Norway AS (i.e., an entity of SATS’ corporate group)³ had transferred their personal data to other companies within its corporate group, as well as to Facebook outside the EU/EEA, without a proper legal ground.⁴ Complainant No 1 also claimed that an access request they submitted on 29 August 2018 to privacy@satselixia.no pursuant to Article 15 GDPR has remained unanswered.⁵

On 1 March 2019, Datatilsynet received another complaint against SATS (Case 20/02422, previously 19/00817).⁶ This complaint was submitted by another member of the fitness centers run by SATS in Norway (hereinafter “Complainant No 2”) who essentially claimed that SATS failed to respond to an access request they submitted on 25 February 2019 pursuant to Article 15 GDPR, and refused to comply with an erasure request they submitted on the same date pursuant to Article 17 GDPR, after they had their membership terminated by SATS.⁷

On 7 October 2019, Datatilsynet received yet another complaint against SATS (Case 20/01707, previously 19/03020).⁸ This complaint was submitted by another member of the fitness centers run by SATS in Norway (hereinafter “Complainant No 3”) who essentially claimed that SATS refused to comply with an erasure request they submitted to SATS on 5 October 2019 pursuant to Article 17 GDPR, after they had their membership terminated by SATS.⁹

² See letter to Datatilsynet dated 2 October 2018 (hereinafter “Complaint No 1”).

³ When the complaint was lodged with Datatilsynet SATS Norway AS was named HFN Norway AS.

⁴ See Complaint No 1.

⁵ Ibid.

⁶ See email to Datatilsynet dated 1 March 2019 (hereinafter “Complaint No 2”).

⁷ Ibid.

⁸ See email to Datatilsynet dated 7 October 2019 (hereinafter “Complaint No 3”).

⁹ Ibid.

On 7 September 2021 and 5 October 2021, Datatilsynet formally approached SATS and asked the company to express its views on the issues raised in Complaint No 2 and Complaint No 3.¹⁰ We received SATS' replies on 1 December 2021.¹¹

On 8 December 2021, Datatilsynet received one more complaint against SATS (Case 21/04061).¹² This complaint was submitted by yet another member of the fitness centers run by SATS in Norway (hereinafter "Complainant No 4") who essentially claimed that SATS refused to comply with an erasure request they submitted on 6 August 2021 pursuant to Article 17 GDPR.

On 23 March 2022, Datatilsynet sent further questions to SATS on all of the above complaints.¹³ We received SATS' response on 28 April 2022.¹⁴

Given that all of the above complaints concerned partially similar alleged infringements of data subjects' rights committed by SATS, Datatilsynet decided to handle all of these complaints jointly, also for reasons of procedural efficiency. Moreover, as the GDPR and its novel international data transfer requirements became applicable in Norway on 20 July 2018, Datatilsynet decided not to investigate the part of Complaint No 1 dealing with an alleged unlawful transfer of personal data that took place in May 2018 (or earlier).¹⁵ However, this is without prejudice to the possibility of opening future inquiries into SATS' compliance with data transfer requirements.

After having investigated all of these complaints, on 26 September 2022, Datatilsynet sent SATS an advance notification of its intention to issue an administrative fine of NOK 10 000 000 (ten million) against SATS for having violated several provisions of the GDPR.¹⁶

On 31 October 2022, SATS submitted written representations to Datatilsynet regarding the contested violations and envisaged administrative fine. The present decision takes account of such written representations.¹⁷ However, in our view, SATS' submissions do not warrant any significant changes in our assessment of the present case, as outlined in further detail below.

On 30 December 2022, Datatilsynet submitted a draft decision—which was in line with the above advance notification—to the other supervisory authorities concerned in accordance with Article 60(3) GDPR. None of the other supervisory authorities concerned expressed a relevant and reasoned objection to the draft decision within four weeks after having been consulted by Datatilsynet. Thus, Datatilsynet is bound by that draft decision,¹⁸ which is mirrored in the present decision.

¹⁰ See Datatilsynet's letters to SATS dated 7 September and 5 October 2021.

¹¹ See SATS' letters to Datatilsynet dated 1 December 2021.

¹² See email to Datatilsynet dated 8 December 2021 (hereinafter "Complaint No 4").

¹³ See Datatilsynet's letter to SATS dated 23 March 2022.

¹⁴ See SATS' letter to Datatilsynet dated 28 April 2022.

¹⁵ See also Article 57(1)(f) GDPR, which specifies that supervisory authorities should investigate complaints "to the extent appropriate".

¹⁶ See Datatilsynet's letter to SATS dated 26 September 2022.

¹⁷ See SATS' letter to Datatilsynet dated 31 October 2022.

¹⁸ See Art. 60(6) GDPR.

4. Legal Background

4.1. Scope of Application of the GDPR

Under Article 2(1) GDPR, the Regulation:

“[...] applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.”

Moreover, Article 3(1) GDPR provides that the Regulation:

“[...] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.”

4.2. Definitions

The GDPR lays down the following definitions, which are relevant in the present case:

Pursuant to Article 4(1) GDPR:

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

Pursuant to Article 4(2) GDPR:

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

Pursuant to Article 4(7) GDPR:

“‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.”

Pursuant to Article 4(11) 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.”

Pursuant to Article 4(16) GDPR:

“‘main establishment’ means:

(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 of personal data 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; [...].”

Pursuant to Article 4(23) GDPR:

“‘cross-border processing’ means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.”

4.3. Lawfulness of Processing, Information Obligations and Data Subjects’ Rights

Article 5(1) GDPR reads as follows:

“I. Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');*

- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken 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');
- (e) 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');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Moreover, Article 6(1) GDPR reads:

"1. 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. [...]"

Further, Article 12(1) and (3) GDPR reads:

“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.

[...]

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.”

Article 13(1)(c) and (2)(a) GDPR provides:

“1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

[...]

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

[...]

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period [...].”

Furthermore, Article 15 GDPR reads:

“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.”

In addition, Article 17 GDPR reads:

“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 the personal data, the controller, taking account of available technology and the cost of 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 links to, or copy or replication of, those personal data.*

3. *Paragraphs 1 and 2 shall not apply to the extent 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) as well as Article 9(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.”*

4.4. Competence, Tasks and Powers of Supervisory Authorities under the GDPR

Pursuant to Article 55(1) GDPR:

“Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.”

Further, Article 56(1) GDPR reads as follows:

“Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.”

Pursuant to Article 58(2) GDPR:

“2. Each supervisory authority shall have all of the following corrective powers:

- (a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;*
- (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;*
- (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;*
- (e) to order the controller to communicate a personal data breach to the data subject;*
- (f) to impose a temporary or definitive limitation including a ban on processing;*
- (g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;*
- (h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;*

- (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;
- (j) to order the suspension of data flows to a recipient in a third country or to an international organisation.”

Pursuant to Article 83(1) to (5) GDPR:

- “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.

3. 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.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

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 pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). [...]”

4.5. EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area (“EEA”) Agreement by means of Decision of the EEA Joint Committee No 154/2018 (“EEA Joint Committee Decision”).¹⁹

Article 1(b) of the EEA Joint Committee Decision provides that:

“[...] the terms “Member State(s)” and “supervisory authorities” shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.”

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

“References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.”

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.²⁰ The Personal Data Act and the GDPR became applicable in Norway on 20 July 2018.²¹

5. Datatilsynet’s Competence

SATS runs a chain of fitness centers. It has its headquarter in Norway, but has also operations and offices in Denmark, Finland and Sweden.²²

Thus, SATS has several establishments in the EU/EEA, including in Norway, and in the context of the activities of these establishments it processes personal data, including the personal data of its customers (i.e., the about 700 000 members of its fitness centers), such as the complainants. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of the complainants, SATS (i.e., the controlling undertaking of the SATS group) qualifies as a controller (within the meaning of Article 4(7) GDPR), as it is SATS that had a factual influence on and decided the means and

¹⁹ Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

²⁰ Act No 38 of 15 June 2018 relating to the processing of personal data (“personopplysningsloven”).

²¹ Ibid., § 32.

²² See SATS’ letter to Datatilsynet dated 28 April 2022.

purposes of the relevant personal data processing, as acknowledged in SATS' privacy policy.²³ The company has not disputed SATS' controller status in the context of Datatilsynet's inquiry.²⁴

As a controller, SATS has its main establishment (within the meaning of Article 4(16) GDPR) in Norway.²⁵ Moreover, the processing of the personal data of SATS members, including the complainants, qualifies as cross-border processing under Article 4(23) GDPR. This is because, although all complainants are members of SATS' fitness centers in Norway, SATS members' personal data may be accessed by SATS' staff in all of the European countries in which SATS operates, and SATS' internal routines and policies on data storage, erasure and access are the same in all of the European countries in which SATS operates.²⁶

Therefore, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case, and Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. This was not disputed by SATS in the course of our inquiry.²⁷

6. Datatilsynet's Assessment

6.1. Findings of a Violation of Articles 12(3) and 15 GDPR

The evidence collected by Datatilsynet shows that Complainant No 1 and Complainant No 2 each submitted an access request to SATS, on 29 August 2018 and 25 February 2019.²⁸ Both requests were explicit in demanding either information on the recipients of the complainant's personal data and the legal ground for sharing their personal data with such recipients,²⁹ or a copy of the personal data of the complainant.³⁰ In this regard, it should be noted that, in order to make an access request under the GDPR, it is sufficient for the requesting data subjects to specify that they want to obtain information on the processing of their personal data, and it is

²³ See SATS' privacy policy from September 2021 (attached to Complaint No 4), which states (in Norwegian): "Denne personvernklæringen er ment å gi informasjon om hvordan og hvorfor SATS Group AS («SATS Group») samler inn og behandler personopplysninger. Det er SATS Group v/CEO som er behandlingsansvarlig for opplysninger som samles inn og behandles av SATS Group." Note that, on 11 October 2022, SATS' Nordic Head of Legal & Compliance informed us that SATS Group AS does not exist any longer, and that all correspondence should instead be addressed to SATS ASA.

²⁴ Cf. SATS' letters to Datatilsynet dated 1 December 2021, 23 March 2022, 28 April 2022 and 31 October 2022.

²⁵ See SATS' letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): "SATS har sin hovedadministrasjon i Oslo og den aktuelle behandlingen blir utført fra samme sted, slik at «hovedvirksomheten» er i Norge i personvernforordningens forstand").

²⁶ See SATS' letter to Datatilsynet dated 28 April 2022.

²⁷ Cf. SATS' letter to Datatilsynet dated 31 October 2022.

²⁸ See correspondence attached to Complaint No 1 and Complaint No 2.

²⁹ See Complainant No 1's email to privacy@satselixia.no dated 29 August 2018 (stating: "I would like to receive information on the parties that my personal data has been shared with, categories of data sent to those parties, as well as legal grounds for such sharing").

³⁰ See Complainant No 2's email to SATS' Customer Service Manager (i.e., the SATS' employee who notified them of the revocation of their SATS membership) dated 25 February 2019 (stating: "Personopplysninger skal være forsvarlig innhentet og korrekt, men her bygger Sats utestellelsen alene på betjeningen sin versjon av saken uten kontradiksjon. Dette er i strid med personopplysningsloven. Jeg ber derfor om innsyn og kopi av samtlige opplysninger i sakens anledning med; innhold, dato og klokkeslett").

not necessary to specify the legal basis of the request.³¹ Further, both requests were submitted through communication channels made available by SATS for similar inquiries.³² In this respect, it should be pointed out that if a data subject makes a request using a communication channel provided by the controller, such request should be considered effective and the controller should handle such a request accordingly.³³ Therefore, the access requests at hand were effective and validly submitted for the purpose of Article 15 GDPR.

When Datatilsynet asked SATS whether it responded to such access requests, SATS replied that it was unable to confirm that it had taken action with respect to the access request submitted by Complainant No 1.³⁴ SATS further confirmed this in the written representations it sent to Datatilsynet on 31 October 2022.³⁵ This is despite the fact that Complainant No 1 sent several reminders to SATS.³⁶ In essence, according to the evidence collected by Datatilsynet, that access request has remained unanswered to this date.

In its written representations, SATS argued that it is arbitrary from the part of Datatilsynet to contest a violation of Articles 12(3) and 15 GDPR due to a failure to respond to an access request that was submitted around a month after the GDPR became applicable in Norway, as at that time many companies experienced challenges in applying the new rules.³⁷ We take note of this argument, but find it untenable. As acknowledged by SATS itself, the fact that other companies faced challenges with adapting to the GDPR after it became applicable in 2018 is not a valid justification for a violation of the GDPR that started to occur in September 2018.³⁸ Moreover, it should be stressed that SATS has never replied to the access request of Complainant No 1—not even after Datatilsynet contacted SATS in connection with Complainant No 1—with the result that that violation is still ongoing, and therefore it does not only concern SATS’ failure to act in 2018. Further, it should be noted that Norwegian data subjects enjoyed a right of access also under the Norwegian Data Protection Act from 2000, which was in force before the GDPR became applicable in Norway.³⁹ Thus, this was not a completely new right that SATS had to become familiar with only after the GDPR became applicable; the company should have had appropriate routines in place to timely respond to access requests since 2001.⁴⁰ In passing, it should be emphasized that Datatilsynet’s enforcement action in the present case

³¹ EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, para. 50.

³² That is the email privacy@satselia.no, and the email address of SATS’ Customer Service Manager who notified to Complainant No 2 the termination of their membership.

³³ EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, paras. 52-57.

³⁴ See SATS’ letter to Datatilsynet dated 28 April 2022.

³⁵ See SATS’ letter to Datatilsynet dated 31 October 2022 (stating (in Norwegian): “SATS erkjenner at man ikke kan dokumentere svaret på innsynsforespørslene fra klager 1”).

³⁶ See correspondence attached to Complaint No 1.

³⁷ See SATS’ letter to Datatilsynet dated 31 October 2022.

³⁸ Ibid. (stating (in Norwegian): “Det bør bemerkes at forespørslene kom én måned etter GDPR trådte i kraft. SATS var på den tiden ikke alene med å ha utfordringer med å implementere og operasjonalisere sine nye personvernrutiner. SATS forstår at det i utgangspunktet ikke er unnskyldende, men [...]” (emphasis added)).

³⁹ Cf. Sections 16 and 18 of the Norwegian Data Protection Act (LOV-2000-04-14-31) (repealed).

⁴⁰ Cf. Section 50 of the Norwegian Data Protection Act (LOV-2000-04-14-31) (repealed). It should be noted that Complainant No 1 submitted an access request also under the rules in force before July 2018. See the correspondence attached to Complaint No 1.

was triggered by complaints submitted by data subjects—which Datatilsynet is required to investigate to the extent appropriate and with all due diligence⁴¹—and it is not the result of an “arbitrary” *ex officio* initiative aimed at singling out SATS’ state of compliance.

As for the second access request, SATS first responded that it did not receive any access request from Complainant No 2,⁴² and later noted that it responded to the access request of Complainant No 2 on 27 February 2019.⁴³ Further, in its written representations, SATS acknowledged that it did not respond satisfactorily to the access request from Complainant No 2.⁴⁴ However, the company noted that the request from Complainant No 2 was handled, half a year after the GDPR became applicable in Norway, by SATS’ customer service, which at that time was probably less aware of GDPR requirements than others within the organization; something that—according to SATS—was common to most Norwegian companies at the time.⁴⁵ We take note of this argument, but find it unconvincing. At the outset, it should be noted that there were approximately two years between the entry into force of the GDPR in 2016⁴⁶ and the moment in which it started to apply in 2018.⁴⁷ Therefore, companies had at least two years to adapt to the new rules, and European supervisory authorities have repeatedly stated that there would be no “grace period” after the GDPR became applicable in 2018.⁴⁸ Moreover, as previously noted, the alleged similar challenges experienced by other businesses with the implementation of the GDPR are no valid excuse for a violation committed by SATS. Moreover, as part of its accountability duties,⁴⁹ it was SATS’ responsibility to ensure that its personnel in charge of handling customers’ inquiries was sufficiently aware of and trained to comply with data subjects’ rights, also in view of the fact that—as noted above—the right of access was not a completely new right introduced by the GDPR.

At any rate, in Datatilsynet’s view, SATS did not take adequate action in response to the access request from Complainant No 2 without undue delay. Most notably, it did not provide any information on action taken on the request to receive a copy of their personal data that Complainant No 2 submitted to SATS.⁵⁰ The email that SATS sent to Complainant No 2 on 27 February 2019 was mainly a response to the complainant’s erasure request (see section 6.2 below), and did not provide all of the information that the data subject requested and was

⁴¹ See Article 57(1)(f) GDPR. See too CJEU, Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, para. 109.

⁴² See SATS’ letter to Datatilsynet dated 1 December 2021 (stating (in Norwegian): “SATS har ikke registrert å ha mottatt en anmodning om innsyn”).

⁴³ See SATS’ letter to Datatilsynet dated 28 April 2022.

⁴⁴ See SATS’ letter to Datatilsynet dated 31 October 2022 (stating (in Norwegian): “SATS erkjenner også at man ikke svarte fullgodt på innsynsforespørselen fra klager 2”).

⁴⁵ Ibid.

⁴⁶ See Art. 99(1) GDPR.

⁴⁷ See Art. 99(2) GDPR and § 32 personopplysningsloven.

⁴⁸ See e.g.: <<https://www.theparliamentmagazine.eu/news/article/gdpr-no-period-of-grace-following-entry-into-force>>; <<https://www.natlawreview.com/article/happy-gdpr-day>>.

⁴⁹ See Arts. 5(2) and 24 GDPR.

⁵⁰ In this regard, it should be noted that the EDPB has opined that “The controller shall react and, as a general rule, provide the information under Art. 15 without undue delay, which in other words means that the information should be given as soon as possible. This means that, if it is possible to provide the requested information in a shorter amount of time than one month, the controller should do so.” See EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, para. 156.

entitled to receive under Article 15 GDPR.⁵¹ That email simply provided a brief description of the incident that led to the termination of the SATS membership of Complainant No 2, and a small extract of some parts of SATS' general terms and conditions, as well as information on SATS' internal data retention policy regarding the personal data of banned members. In this regard, it should be noted that "the controller should always be able to demonstrate, that the way to handle the request aims to give the broadest effect to the right of access and that it is in line with its obligation to facilitate the exercise of data subjects rights"⁵² and that "the notion of a copy has to be interpreted in a broad sense".⁵³ In its written representations, SATS took issue with the fact that, in its advance notification of an administrative fine, Datatilsynet referred to the latter two passages in the EDPB's Guidelines 01/2022 on the right of access, which—according to SATS—do not reflect the wording of the GDPR, although SATS did not explain why.⁵⁴ In this respect, Datatilsynet notes that, although they are not binding, EDPB guidelines are important interpretative aids⁵⁵ that supervisory authorities should take into account to make sure that they comply with their legal obligation to ensure the consistent application of the GDPR throughout the EU/EEA.⁵⁶ Further, in our view, the statements made in such passages directly follow from the obligation to facilitate the exercise of data subjects rights set out in Article 12(2) GDPR, as well as from the broad effect that should be given to the data subject's right of access so as to ensure that such a right "retains its effectiveness" and to "enable the data subject to check [...] that the data concerning him or her are accurate", which implies that the "the information provided must be as precise as possible".⁵⁷ This is also because Article 15 "gives specific expression" to the individual right to access data concerning him or her, enshrined in the second sentence of Article 8(2) of the Charter of Fundamental Rights of the European Union,⁵⁸ as well as Article 8 ECHR.⁵⁹ In any event, it should be stressed that SATS did not provide any copy whatsoever—narrow or broad—of the personal data it processed, as expressly requested by Complainant No 2 and required by Article 15(3) GDPR.

⁵¹ Cf. SATS' Customer Service Manager's email to Complainant No 2 dated 27 February 2019 (attached to Complaint No 2).

⁵² EDPB, Guidelines 01/2022 on data subject rights - Right of access, Version 1.0, Adopted on 18 January 2022, para. 35.

⁵³ Ibid., para. 25.

⁵⁴ See SATS' letter to Datatilsynet dated 31 October 2022.

⁵⁵ EDPB guidelines are even used as interpretative aids by European high courts. See e.g. CJEU, Case C-645/19, *Facebook Ireland and Others*, para. 74; CJEU, Case C-911/19, ECtHR, *Biancardi v. Italy, Application no. 77419/16*, judgment of 25 November 2021, paras. 29 and 53.

⁵⁶ See Arts. 51(2) and 70(1)(d)-(m). See too, by analogy, CJEU, Case C-911/19, *Fédération bancaire française (FBF) v Autorité de contrôle prudentiel et de résolution (ACPR)*, para. 71.

⁵⁷ Opinion of Advocate General Pitruzzella in Case C-154/21, *RW v Österreichische Post AG*, paras. 19 and 26.

⁵⁸ Ibid., para. 14.

⁵⁹ ECtHR, *K.H. and Others v. Slovakia*, App. No. 32881/04, para. 47.

Finally, it should be pointed out that SATS acknowledged that its handling of both of the above access requests was not entirely satisfactory,⁶⁰ and that such requests could have been better handled.⁶¹

In light of the above, SATS violated Articles 12(3) and 15 GDPR with respect to Complainant No 1 and Complainant No 2, as it failed to take adequate action on the access requests they submitted on 29 August 2018 and 25 February 2019 within the deadline set out in Article 12(3).

In its written submissions, SATS argued that Datatilsynet's conclusion that SATS violated both Article 12(3) and 15 GDPR would violate the principle of *ne bis in idem* (in Norwegian "dobbeltstraff").⁶² This argument should be rejected. At the outset, it should be recalled that "the principle *ne bis in idem* [...] do[es] not apply to a situation in which several penalties are imposed in a single decision, even if those penalties are imposed for the same actions. In fact, where the same conduct infringes several provisions punishable by fines, the question whether several fines may be imposed in a single decision falls not within the scope of the principle *ne bis in idem*".⁶³ Indeed, neither that principle nor the principle governing concurrent offences "preclude an undertaking from being penalised for an infringement of several distinct legal provisions, even if those provisions have been infringed by virtue of the same conduct."⁶⁴ This is even specifically envisaged in Article 83(3) GDPR, which provides that "[i]f a controller [...] 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" (emphasis added). In any event, Articles 12(3) and 15 GDPR must necessarily be read (and applied) together—and may thus be cumulatively violated—as the first provision regulates the timing for taking action on an access request, whereas the second provision establishes what kind of information must be provided in response to such a request.

6.2. Findings of a Violation of Articles 5(1)(e), 12(3) and 17 GDPR

The evidence collected by Datatilsynet shows that Complainant No 2, Complainant No 3 and Complainant No 4 each submitted a data erasure request to SATS, on 25 February 2019, 5 October 2019 and 6 August 2021. In its written representations, SATS wrongly claimed that the erasure requests were "only two",⁶⁵ whereas the erasure requests assessed by Datatilsynet were three.⁶⁶

⁶⁰ See SATS' letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): "SATS [er] åpen for at det kan ha skjedd mindre glipper i håndteringen av anmodninger fra de fire klagerne saken gjelder, i relasjon til respons tid og begrunnelser").

⁶¹ See SATS' letter to Datatilsynet dated 31 October 2022 (stating (in Norwegian): "SATS erkjenner at medlemmenes forespørslar kunne vært bedre håndtert").

⁶² Ibid., p. 9.

⁶³ GC, Case T-704/14, *Marine Harvest ASA v European Commission*, para. 344. See too CJEU, Case C-10/18 P, *Mowi ASA v European Commission*.

⁶⁴ GC, Case T-704/14, *Marine Harvest ASA v European Commission*, paras. 370-371. See too GC, Case T-609/19, *Canon v European Commission*, para. 461; CJEU, Case C-10/18 P, *Mowi ASA v European Commission*.

⁶⁵ See SATS' letter to Datatilsynet dated 31 October 2022, p. 3 (stating (in Norwegian): "her er det snakk om kun to forhold").

⁶⁶ See Complaints No 2, No 3 and No 4.

The erasure requests of Complainant No 2 and Complainant No 3 concerned all of their personal data, and were submitted after the termination of their SATS membership by SATS. Conversely, the erasure request of Complainant No 4 was not submitted in connection with any termination of their membership, and concerned only specific kinds of personal data, namely the logs of their training activities.

SATS eventually responded to all of such requests,⁶⁷ although SATS replied for the first time to Complainant No 4 – after a reminder from the complainant⁶⁸ – on 23 September 2021,⁶⁹ i.e. more than one month after it received their request on 6 August 2021, which constitutes in itself a violation of Article 12(3) GDPR.⁷⁰

In its reply to Complainant No 3 dated 11 October 2019, SATS refused to delete the complainant's date of birth, name and picture, and justified this on the basis of the following internal policy, which was copied verbatim (in English) in the text of the email to the complainant:

“If the customer relationship is terminated due to improper behavior from the member, name, date of birth and picture shall be kept for 60 months. Further, the member in question shall be marked as ‘excluded’. The rest of the data shall be deleted, included possible reports on the behavior.”⁷¹

Complainant No 3 was further informed by SATS that, based on the above internal policy, SATS could retain their date of birth, name and picture for 60 months, whereas the rest of their personal data would be deleted within 30 days.⁷² SATS also informed the same complainant that they would be banned from SATS' fitness centers for 24 months from the date in which they received SATS' notification of the termination of their membership.⁷³

Complainant No 2 received a partially similar response. Most notably, in its reply to Complainant No 2 dated 27 February 2019, SATS stated that:

⁶⁷ SATS replied to the erasure requests of Complainants No 2 and No 3 within the deadline set out in Article 12(3) GDPR, but failed to take adequate action upon such requests, as outlined below.

⁶⁸ See Complainant No 4's email to SATS dated 16 September 2021 (attached to Complaint No 4).

⁶⁹ As acknowledged by SATS. See SATS's letter to Datatilsynet dated 28 April 2022.

⁷⁰ Article 12(3) GDPR provides that “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” (emphasis added). Datatilsynet has taken into account the relatively modest duration of SATS' delay when setting the amount of the administrative fine issued against SATS (see Section 7.1 below).

⁷¹ See email from kundeservice@sats.no to Complainant No 3 dated 11 October 2019 (attached to SATS' letter to Datatilsynet dated 1 December 2021).

⁷² Ibid.

⁷³ Ibid. (stating (in Norwegian): “du vil være utestengt fra SATS i 24 måneder fra dato vi sendte deg informasjon om utestengelsen per brev”).

“Banned members can, in accordance with the GDPR, request to have their training history deleted, while other information and the member profile itself can be retained by us for up to 60 months”.⁷⁴

SATS also informed Complainant No 2 that they would be banned from SATS’ fitness centers for one year starting from 21 February 2019.⁷⁵

When asked by Datatilsynet to explain the purposes for which SATS retained and processed the personal data of banned members (including Complainant No 2 and Complainant No 3), SATS stated:

“SATS processes the date of birth, name and photo [of the former member] in connection with [their] exclusion, with the aim of being able to prevent the excluded member from using SATS’ services during the exclusion period” (emphasis added).⁷⁶

After having been notified of our intention to issue an administrative fine, SATS (knowingly)⁷⁷ changed position, and stated that a broader and vaguer purpose applies in this context: “the purpose of the storage is to be able to process the information in connection with the ban. This purpose does not expire as soon as the ban is lifted”.⁷⁸ It also claimed that such a change of position would not affect the assessment of the legitimacy of the retention period.⁷⁹ We disagree with the latter claim: any broadening of the scope of the purpose of a processing operation inevitably affects such an assessment. This is because personal data must be kept for “no longer than is necessary for the purposes for which the personal data are processed”⁸⁰ (emphasis added), with the result that the necessity of the retention must be assessed vis-à-vis the relevant purpose. Furthermore, it is not possible to adjust the relevant purpose *ex post*; the assessment should be made with respect to the purpose identified by the controller at the outset of the relevant processing, as it results from the evidence collected by the supervisory authority during its investigation. Moreover, the answer that SATS provided to Datatilsynet in April 2022 specifically addressed the purpose of processing the personal data of Complainant No 2 and Complainant No 3—which SATS identified as “being able to prevent the excluded member from using SATS’ services during the exclusion period”—whereas in its written representations from October 2022 SATS described the purpose of processing the personal data of banned members in general. In this respect, Datatilsynet acknowledges that, in certain exceptional

⁷⁴ SATS’ email to Complainant No 2 dated 27 February 2019 (our translation) (stating (in Norwegian): “Utestengte medlemmer kan i henhold til GDPR be om å få sin treningshistorikk slettet, mens annen informasjon og selve medlemsprofilen kan beholdes av oss i inntil 60 måneder”).

⁷⁵ SATS’ email to Complainant No 2 dated 21 February 2019 (stating (in Norwegian): “Du er utestengt for 1 år fra dagens dato”).

⁷⁶ See SATS’ letter to Datatilsynet dated 28 April 2022 (our translation) (stating (in Norwegian): “SATS behandler fødselsdato, navn og bilde i forbindelse med utestengelse, for det formål å kunne forhindre det utestengte medlemmet fra å benytte seg av SATS’ tjenester i løpet av utestengelsesperioden”).

⁷⁷ See SATS’ letter to Datatilsynet date 31 October 2022, p. 3 (stating (in Norwegian): “SATS beklager at formålet er noe snevrere angitt i SATS’ svar av 28. april 2022 til Datatilsynet”).

⁷⁸ Ibid. (stating (in Norwegian): “[...] er formålet med oppbevaringen å kunne behandle opplysningene i forbindelse med utestengelsen. Dette formålet utløper ikke straks utestengelsen er opphevet”).

⁷⁹ Ibid. (stating (in Norwegian): “dette har naturligvis ingenting å si for den rettslige vurderingen av om oppbevaringstiden er legitim”).

⁸⁰ See Art. 5(1)(e) GDPR.

circumstances, SATS may need to process the personal data of banned members for purposes that go beyond preventing them from using SATS' services during the exclusion period (e.g. to defend a legal claim in court, etc.). However, this would not apply invariably in all cases, and most importantly it does not apply in this case, given that, when asked about the purpose for which SATS processed the data of Complainant No 2 and Complainant No 3, SATS replied that it processed such data to be "able to prevent the excluded member from using SATS' services during the exclusion period". Therefore, in the present case, Datatilsynet will exclusively focus on the latter purpose.

A company running a fitness center may legitimately retain and refuse to delete the date of birth, name and photo of former members who were banned from its fitness center for the entire duration of the relevant ban. This is because such information is essential to enable the center's staff to enforce the ban. However, retaining such personal data for a period longer than the duration of the ban, or retaining more than the aforementioned personal data (e.g., training logs, correspondence, etc.), violates the storage limitation principle set out in Article 5(1)(e) GDPR (unless the data are retained for other legitimate purposes beyond preventing the excluded member from using the center's services during the exclusion period). This is because the personal data at hand would no longer be necessary for the purposes for which they are/were processed.

Whether SATS legitimately refused to act – at least partially – upon the erasure requests submitted by Complainant No 2 and Complainant No 3 should also be assessed in light of the actual necessity of processing their data, as the GDPR's right of erasure applies *inter alia* where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.⁸¹

In the present case, in our view, SATS failed to comply with Articles 17 and 5(1)(e) GDPR with respect to the personal data of both Complainant No 2 and Complainant No 3.

Despite the fact that Complainant No 3 required the erasure of all of their personal data on 5 October 2019, and that SATS informed them on 11 October 2019 that their personal data other than their date of birth, name and picture would be deleted within 30 days, SATS deleted Complainant No 3's training logs, membership number, address, telephone number and e-mail only on 4 November 2021,⁸² after the opening of Datatilsynet's inquiry. In this regard, it should be noted that "SATS acknowledges that certain member data on complainant [...] No 3 were stored beyond SATS' internal routines".⁸³ Thus, with respect to the erasure of such data, SATS did not take action without undue delay, as required by Article 17(1) GDPR.

Moreover, SATS retained the date of birth, name and picture of Complainant No 3 beyond the relevant exclusion period of 24 months—as such data were deleted on 4 November 2021 (i.e., after Datatilsynet's inquiry) and the exclusion period started running on 4 October 2019—even though such data were processed "with the aim of being able to prevent the excluded member

⁸¹ See Art. 17(1)(a) GDPR.

⁸² See SATS' letter to Datatilsynet dated 28 April 2022.

⁸³ See SATS' letter to Datatilsynet dated 31 October 2022, p. 3 (stating (in Norwegian): "erkjenner SATS at visse medlemsdata om klager [...] ble lagret utover SATS' internrutiner.").

from using SATS’ services during the exclusion period”, with the result that such data were retained for longer than it was necessary for the purpose for which the data were processed, in breach of Article 5(1)(e) GDPR.

Similarly, despite the fact that Complainant No 2 required the erasure of all of their personal data on 25 February 2019, and that the above-cited SATS’ internal policy provides that personal data other than the date of birth, name and picture “shall be deleted” after the member’s exclusion, SATS retained the “address and telephone number”⁸⁴ of Complainant No 2 until 4 November 2021.⁸⁵ It also retained the correspondence with Complainant No 2, at least until 2021.⁸⁶ In this respect, it should be noted that “SATS acknowledges that certain member data on complainant No 2 [...] were stored beyond SATS’ internal routines”.⁸⁷ SATS claimed that this was likely due to a mistake, which was presumably due to the extraordinary workload during the Covid-19 pandemic.⁸⁸ However, Datatilsynet finds that the pandemic is an irrelevant factor in this respect, given that the personal data at hand should have been deleted without undue delay from 25 February 2019, i.e. long before the beginning of the pandemic in Norway. Moreover, SATS retained the date of birth, name and picture of Complainant No 2 well beyond the relevant exclusion period of one year, as such data were deleted on 4 November 2021 (i.e., after Datatilsynet’s inquiry) and the exclusion period started running on 21 February 2019. Thus, such data were retained for longer than it was necessary for the purpose for which the data were processed, in breach of Article 5(1)(e) GDPR, given that they were processed “with the aim of being able to prevent the excluded member from using SATS’ services during the exclusion period”.⁸⁹

In its written representations, SATS argued that the assessment of the necessity of a storage period is to a large extent discretionary, and that Datatilsynet is not in the position to and should refrain from questioning the assessment made by the controller.⁹⁰ In this respect, it should be noted that, while it is for the controller to ensure operational compliance with its data retention obligations, the controller must also be able to *demonstrate* compliance with such obligations to the supervisory authority,⁹¹ and thus allow the authority to review whether the retention periods set by the controller are justified. Consequently, Datatilsynet is competent to review the assessment made by the controller to ensure compliance with its retention obligations. In the present case, Datatilsynet has simply reviewed the necessity of the retention of the data of Complainants No 2 and 3 in light of: (1) the relevant purpose of the processing identified by SATS, which is linked to a specific timeframe (“being able to prevent the excluded member from using SATS’ services during the exclusion period” (emphasis added)); and (2) SATS’

⁸⁴ See SATS’ letter to Datatilsynet dated 1 December 2021 (stating (in Norwegian): “Klager ble utestengt fra SATS’ sentre den 20. februar 2019 grunnet truende oppførsel motto av SATS’ ansatte. Utestengelsen ble registrert i SATS’ medlemssystem Exerp. Ved utestengelse lagrer SATS navn, fødselsdato, adresse og telefonnummer”).

⁸⁵ Ibid.

⁸⁶ Excerpts from such correspondence were included by SATS in its reply to Datatilsynet dated 1 December 2021.

⁸⁷ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 3 (stating (in Norwegian): “erkjenner SATS at visse medlemsdata om klager 2 [...] ble lagret utover SATS’ internrutiner.”).

⁸⁸ See SATS’ letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): “ser det ut til a ha skjedd en glipp som antagelig skyldes den ekstraordinære arbeidsmengden under pandemien”).

⁸⁹ See SATS’ letter to Datatilsynet dated 28 April 2022 (our translation).

⁹⁰ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 4.

⁹¹ See Art. 5(2) GDPR.

retention policy, which provided that personal data other than the date of birth, name and picture “shall be deleted” after the member’s exclusion. Moreover, SATS itself has acknowledged that it has retained some of the personal data of Complainants No 2 and 3 for longer than its own internal routines envisaged. Therefore, Datatilsynet has not determined the necessity of the relevant retention periods in the abstract, in light of its own subjective evaluations; it has merely tested the necessity of the relevant retention periods in light of the information and justifications provided by the controller.

In our view, SATS also violated Articles 17 and 5(1)(e) GDPR with respect to Complainant No 4. This is for the reasons outlined below.

As explained in more detail below (see section 6.4), SATS’ general terms and conditions allow its members to withdraw consent to the processing of their training history data and request that such data be deleted. Thus, in our view, Complainant No 4 legitimately relied on this provision to withdraw their consent and request the deletion of their training history data on 6 August 2021:

“Jeg [...] trekker herved tilbake mitt samtykke til at SATS kan behandle, lagre eller på annen måte oppbevare følgende personopplysninger:

- Sporing av hvilket treningssenter jeg trener på
- Sporing av hvilke tidspunkter jeg trener på
- Annen overvåkning av min treningsaktivitet [...]

Vennligst bekreft at dette er mottatt, at ovennevnte personopplysninger vil bli slettet fra og med uke 31, og at ovennevnte personopplysninger ikke vil bli innhentet, lagret, oppbevart eller på andremåter behandlet fra og med uke 31”.⁹²

In light of such request, SATS should have deleted the complainant’s training history data without undue delay in accordance with Article 17(1)(b) GDPR. Instead, SATS replied to Complainant No 4 that the deletion would take place within 6 months in accordance with its privacy policy, and explained that such a deletion deadline was set among other things for ensuring the safety of SATS members and infection tracing during the pandemic.⁹³ SATS also informed Complainant No 4 that Article 17(1)(b) was not applicable to their case, as SATS’ legal basis for processing their training history data was “Article 6(1)(b) and (f)”, and the processing was still necessary in relation to the purposes for which they were collected or otherwise processed.⁹⁴

⁹² See Complainant No 4’s email to privacy@sats.no dated 6 August 2021 (attached to Complaint No 4).

⁹³ See SATS’ email to Complainant No 4 dated 23 September 2021 (stating (in Norwegian): “Sletting skjer i henhold til vårpersonvernerklæring senest etter 6 måneder ved mottatt anmodning om sletting [...] Bakgrunnen for [...] slettefristen på 6 måneder etter mottatt krav om sletting, er blant annet sikkerheten til våre medlemmer samt smittesporing ”).

⁹⁴ See SATS’ email to Complainant No 4 dated 2 October 2021 (stating (in Norwegian): “Vi har tidligere forklart deg grunnlaget for oppbevaringen i inntil seks måneder fra vi har mottatt en sletteanmodning, som – blant andre forhold – er knyttet til sikkerheten til våre medlemmer samt smittesporing. Dette er hensyn som faller innenfor artikkel 17 nr. 1 a) i personvernforordningen (GDPR), som «nødvendige for formålet de ble samlet inn eller behandlet for», sammenholdt med behandlingsgrunnlaget i artikkel 6 nr. 1 bokstav b) og f). Som konsekvens av

In our view, SATS' position on the applicability of Article 6(1)(b), and accordingly on the inapplicability of Article 17(1)(b), is untenable in this case (see further section 6.4 below). Moreover, while the retention for a few months of the training logs of the previous last few weeks or months for infection tracing purposes may be justified in the context of the Covid-19 pandemic, the blanket retention for up to 6 months (after an erasure request) of all available training logs appears unjustified and disproportionate.⁹⁵ Indeed, data retention for infection tracing purposes should be proportionate to the incubation and infectious period of Covid-19, which was deemed to require a quarantine period of 14 days for those who had a close contact with an infected individual in the last 24 hours.⁹⁶ The excessiveness of a retention period of 6 months is further supported, for example, by the fact that the Regulation on Digital Infection Tracing provided for a data retention period of up to 30 days.⁹⁷ While SATS insisted in its written representations that 6 months was a necessary and proportionate retention period, it did not provide any evidence or specific arguments to support its view.⁹⁸ In any event, it should be noted that SATS deleted the training history data of Complainant No 4 only on 7 April 2022, i.e. after the opening of our inquiry and well beyond the 6 months deadline specified by the company.⁹⁹ However, SATS stated that this was due to a mistake.¹⁰⁰

In conclusion, based on the evidence collected by Datatilsynet, it appears that SATS did not properly handle any of the above three erasure requests. In this regard, it should be noted that SATS itself has acknowledged that its handling of these erasure requests was not entirely satisfactory.¹⁰¹ While, if taken in isolation, each of these episodes of mishandling of a data subject's request is not very grave, the fact that they have occurred repeatedly over a long period of time and have affected multiple data subjects is indicative of broader, more systemic issues regarding SATS' handling of data subjects' requests. Moreover, it bears emphasizing that SATS proceeded to delete the personal data of all of the above complainants with a considerable delay, only after Datatilsynet's inquiry. It would have likely retained such data for even longer without our intervention.

at det på denne bakgrunn foreligger et lovlig formål for behandlingen og utsatt sletting, har du heller ikke et krav på omgående sletting i medhold av artikkel 17 nr. 1bokstav b.)".)

⁹⁵ Note that Complainant No 4 has been a member of SATS for about 8 years. Thus, they likely generated a considerable amount of training logs over these years, and SATS' retention of the training logs for infection tracing purposes was not limited to the previous last few weeks or months.

⁹⁶ Forskrift om smitteverntiltak mv. ved koronautbruddet (Covid-19-forskriften). In our guidelines on infection tracing published on 21 September 2020 we wrote that "It will not normally be necessary to store information about visitors for infection control reasons for more than 14 days". See Datatilsynet, Besøksregistrering og smittesporing (21.09.2020) (stating (in Norwegian): "Det vil normalt ikke være nødvendig å lagre opplysninger om besøkende av smittevernghensyn i mer enn 14 dager") <<https://www.datatilsynet.no/personvern-pa-ulike-områder/korona/besøksregistrering-og-smittesporing/>>.

⁹⁷ Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19.

⁹⁸ SATS simply stated (in Norwegian) "SATS' vurdering om lagringstid er uansett rimelig og forsvarlig, og da er det ikke avgjørende om Datatilsynet skulle ha et noe avvikende syn på tidens lengde". Cf. SATS' letter to Datatilsynet dated 31 October 2022, p. 4.

⁹⁹ See SATS' letter to Datatilsynet dated 28 April 2022.

¹⁰⁰ Ibid.

¹⁰¹ See SATS' letter to Datatilsynet dated 28 April 2022 (stating: "SATS [er] åpen for at det kan ha skjedd mindre glipper i håndteringen av anmodninger fra de fire klagerne saken gjelder, i relasjon til respons tid og begrunnelser").

In its written submissions, SATS argued that Datatilsynet's conclusion that SATS breached Articles 5(1)(e), 12(3) and 17 GDPR would violate the principle of *ne bis in idem*.¹⁰² This argument should be rejected. As noted above, that principle does not preclude an undertaking from being penalised for an infringement of several distinct legal provisions, even if those provisions have been infringed by virtue of the same conduct.¹⁰³ Moreover, it should be noted that Article 12(3) and 17 GDPR must necessarily be read (and applied) together—and may thus be cumulatively violated—as the first provision regulates the timing for providing information on the action taken on a request under Article 17, whereas the second provision establishes upon what conditions the right to erasure set out in Article 17 applies.

As for the contested violation of Article 5(1)(e), SATS also argued that “it will always be the case that a breach of a specific obligation [in the GDPR] also represents a breach of one of the privacy principles” and therefore the two breaches should not be cumulated.¹⁰⁴ This argument should be rejected. If one would follow SATS’ argument, a violation of Article 5 should never be contested. However, this would deprive Article 83(5)(a) of essentially any effect, as the latter provision establishes a specific fine for infringements of “the basic principles for processing [...] pursuant to Article 5”.¹⁰⁵ It must be clear that, in our view, the basic principles in Article 5 are both general rules that shall guide the reading of other provisions in the GDPR *and* legal requirements in their own right. In particular, Article 17 should be read jointly and in light of the principle set out in Article 5(1)(e), but the latter provision may also be breached on its own. This has occurred in the present case with respect to the personal data that SATS could legitimately retain for a while after the relevant erasure request (e.g., date of birth, name and photo of banned members), but that it eventually retained for much longer than it was actually necessary. Finally, it should be noted that the EDPB has already found that the same conduct may lead to the simultaneous breach of a principle in Article 5 and of the obligations stemming from that principle in the rest of the GDPR.¹⁰⁶

6.3. Findings of a Violation of Articles 5(1)(a), 12(1), 13(1)(c) and 13(2)(a) GDPR

It is apparent from the evidence collected by Datatilsynet that SATS has established a specific data retention policy with respect to the personal data of members whose membership is terminated by SATS. The policy reads as follows:

“If the customer relationship is terminated due to improper behavior from the member, name, date of birth and picture shall be kept for 60 months. Further, the member in

¹⁰²See SATS’ letter to Datatilsynet dated 31 October 2022, p. 9.

¹⁰³ GC, Case T-704/14, *Marine Harvest ASA v European Commission*, paras. 370-371. See too GC, Case T-609/19, *Canon v European Commission*, para. 461.

¹⁰⁴ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 9 (stating in Norwegian: “Det vil så å si alltid være slik at et brudd på en konkret forpliktelse også representerer brudd på et av personvernprinsippene. Datatilsynet må naturligvis påse at man ikke anser ett og samme forhold som to brudd på GDPR og regner dette dobbelt i sin vurdering av overtredelsesgebyr.”).

¹⁰⁵ See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, para. 191.

¹⁰⁶ See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, paras. 183-201.

question shall be marked as ‘excluded’. The rest of the data shall be deleted, included possible reports on the behaviour”.¹⁰⁷

This policy was apparently developed by SATS in cooperation with an external law firm¹⁰⁸ and appears to be a standard internal policy given that all of SATS’ replies to the erasure requests mentioned above refer to this 60 months retention period, and that the policy at hand was quoted in English in an email in Norwegian to a Norwegian data subject,¹⁰⁹ which—in our view—may indicate that SATS’ customer service copied it from an internal document in English.

Nonetheless, no publicly available documents (including SATS’ privacy policy and terms of service) provide specific information on the retention period at hand, as acknowledged by SATS.¹¹⁰ In this respect, SATS initially noted that the duration of the exclusion of a member may vary and that therefore it is impossible to provide general information on the storage period applicable to the personal data of banned members, and that in any event SATS’ privacy policy mentions that personal data are stored for as long as it is necessary for achieving the purposes for which they are obtained.¹¹¹ However, in its written representations, SATS acknowledged that it should have been more transparent on this point.¹¹²

For the sake of clarity and completeness, Datatilsynet notes that SATS was not sufficiently transparent regarding its data retention policy for the following reasons. First, given that SATS formalized such a retention policy internally, one may not logically argue that it is impossible to inform data subjects of such policy in advance, as this could have been done for example by simply copying the above-quoted wording in SATS’ privacy policy. Secondly, to comply with Article 13(2)(a) GDPR, it is not sufficient to state that personal data will be stored for as long as necessary, without providing any additional information that would enable the data subject to assess, on the basis of their own situation, the retention period for specific data or purposes.¹¹³

Therefore, in our view, SATS violated Articles 5(1)(a) and 13(2)(a) GDPR, as it failed to ensure transparency about the period for which it stores the personal data of banned members and/or the criteria used to determine that period. Under Article 13(1) GDPR, such information should have been provided “at the time when personal data are obtained”. Therefore, it is not sufficient to inform data subjects about this retention period when SATS notifies them of the termination of their membership.

On a general note, Datatilsynet has strong reservations about a blanket storage period of 60 months for personal data of banned members. This is because 60 months is an extraordinarily

¹⁰⁷ See email from kundeservice@sats.no to Complainant No 3 dated 11 October 2019 (attached to SATS’ letter to Datatilsynet dated 1 December 2021).

¹⁰⁸ Ibid. See too SATS’ letter to Datatilsynet dated 31 October 2022, p. 5.

¹⁰⁹ See email from kundeservice@sats.no to Complainant No 3 dated 11 October 2019 (attached to SATS’ letter to Datatilsynet dated 1 December 2021).

¹¹⁰ See SATS’ letter to Datatilsynet dated 28 April 2022.

¹¹¹ Ibid.

¹¹² See SATS’ letter to Datatilsynet dated 31 October 2022, p. 5 (stating in (Norwegian) “På dette punktet tar SATS selvkritikk. [...] Det er på det rene at slettetidene skulle vært mer konkrete”).

¹¹³ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, As last Revised and Adopted on 11 April 2018), p. 38.

long period, which in practice may lead SATS to retain such data for longer than it is necessary, in violation of Article 5(1)(e), as exemplified by how SATS handled the erasure of the data of Complainant No 2 and Complainant No 3 (see section 6.2 above). A retention period of 60 months would only be justifiable in very exceptional circumstances, whereas much shorter retention periods should apply in standard cases. Thus, specific criteria should be set out, and communicated in advance to data subjects, to ensure that the data of banned members are not processed for longer than it is actually necessary in practice, in light of the circumstances of the specific termination of the membership. However, it is for the controller to identify and apply the relevant criteria.

Moreover, SATS' privacy policy in effect in 2021 simply stated that SATS' legal basis for processing the personal data of its customers was generally "performance of a contract" and in some cases "consent" (see further section 6.4 below).¹¹⁴ However, the policy did not clarify which processing activities or purposes were covered by each of these legal bases. This constitutes in itself a breach of Articles 12(1) and 13(1)(c) GDPR, as the information on legal bases in the privacy policy was not "clear" and did not allow data subjects to assess, on the basis of their own situation, what legal basis/purposes apply.¹¹⁵ This confusion was further exacerbated by the fact that, when questioned about the applicable legal basis by a data subject, SATS also referred to a legal basis (i.e., legitimate interest) that was not mentioned among the relevant legal bases listed in its privacy policy.¹¹⁶ Nonetheless, SATS' current privacy policy (updated after the opening of our inquiry) is clearer on this point.¹¹⁷ In its written representations, SATS acknowledged that "the description [in its privacy policy in effect in 2021] of the legal grounds should have been more refined".¹¹⁸ However, it claimed that the recent update to its privacy policy was not triggered by Datatilsynet's inquiry.¹¹⁹

In its written representations, SATS argued that Datatilsynet's conclusion that SATS breached Articles 5(1)(a), 12(1), 13(1)(c) and 13(2)(a) GDPR would violate the principle of *ne bis in idem*.¹²⁰ Moreover, SATS argued that "all violations of Article 13 automatically constitute a breach of Article 12" and that "it will always be the case that a breach of a specific obligation

¹¹⁴ See Personvernerklæring og informasjonskapsler – SATS (attached to Complaint No 4).

¹¹⁵ Cf. Article 29 Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, As last Revised and Adopted on 11 April 2018), page 9.

¹¹⁶ See correspondence attached to Complaint No 4.

¹¹⁷ See: <<https://www.sats.no/legal/personvernerklaring>> (stating: "Vi må ha behandlingsgrunnlag etter GDPR for vår behandling av personopplysninger. For *administrasjon av medlemskap, treningsoppfølging, online trening, app-funksjoner og treningsrelaterte tjenester* er grunnlaget at det er nødvendig for å oppfylle vår avtale med deg. For *kjøp* er det nødvendigheten av å oppfylle en rettslig forpliktelse. For *produktutvikling* er det vår berettigede interesse i forbedring og innovasjon. For *studier* er det vår berettigede interesse å bidra til forskning og folkeopplysning. For *kameraovervåkning* er det behovet for å forebygge farlige situasjoner og å ivareta hensynet til våre ansatte og medlemmers sikkerhet. Om det er nødvendig for oss å behandle særige kategorier av personopplysninger (sensitive personopplysninger) for å yte våre tjenester til deg, er behandlingsgrunnlaget ditt samtykke som du gir via medlemsvilkårene (GDPR artikkel 6 nr. 1 bokstav a og artikkel 7 nr. 4).").

¹¹⁸ See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating in (Norwegian) "På dette punktet tar SATS selvkritikk. [...] beskrivelsen av behandlingsgrunnlagene skulle vært mer raffinert").

¹¹⁹ Ibid.

¹²⁰ See SATS' letter to Datatilsynet dated 31 October 2022, p. 9.

[in the GDPR] also represents a breach of one of the privacy principles”.¹²¹ Therefore, according to SATS, these breaches should not be cumulated. These arguments should be rejected. As noted above, the principle of *ne bis in idem* does not preclude an undertaking from being penalised for an infringement of several distinct legal provisions, even if those provisions have been infringed by virtue of the same conduct.¹²² Moreover, it should be noted that Articles 12(1) and 13 must be read (and applied) together—and may thus be cumulatively violated—as the first provision regulates *how* certain information must be provided, whereas the second provision establishes *what* information must be provided.

As for the violation of the transparency principle in Article 5(1)(a), we emphasize once again that there is nothing in the GDPR that precludes a controller from being penalized both for an infringement of a principle in Article 5 and an infringement of the obligations stemming from that principle in the rest of the GDPR.¹²³ In the present case, by failing to provide sufficient information about the relevant storage periods and legal basis for the processing, SATS has not only violated the specific information requirements laid down in Article 13(1)(c) and (2)(a) GDPR; it also failed to ensure that “personal data [are] processed [...] in a transparent manner in relation to the data subject”, as required pursuant to Article 5(1)(a) GDPR.

6.4. Findings of a Violation of Articles 5(1)(a) and 6(1) GDPR

Complainant No 4 lodged their complaint with Datatilsynet, partly due to their doubts regarding SATS’ position on the legal basis for the processing and storage of training history data.¹²⁴ We believe that Complainant No 4 has raised legitimate doubts regarding SATS’ position on such legal basis. This is due to the fact that SATS’ privacy policy and general terms and conditions provide confusing and misleading information on this point. Furthermore, SATS has provided partially different responses regarding the legal basis for the processing of training history data to Complainant No 4 and to Datatilsynet. This warrants an assessment of whether SATS relied on a valid legal basis for processing training history data.

SATS’ privacy policy in effect in 2021 stated the following with respect to the legal bases that SATS relied on for processing the personal data of its customers:

“RETTSIG GRUNNLAG FOR BEHANDLING AV PERSONOPPLYSNINGER

Behandling av personopplysninger er ikke tiltatt med mindre det foreligger et gyldigbehandlingsgrunnlag. Et slikt behandlingsgrunnlag kan eksempelvis være samtykke fra den registrerte, kontrakt (inngåelse av avtale), lov eller at vi som

¹²¹ Ibid. (stating (in Norwegian): “Det vil så å si alltid være slik at et brudd på en konkret forpliktelse også representerer brudd på et av personvernprinsippene [...] alle brudd på artikkel 13 automatisk utgjør brudd på artikkel 12”).

¹²² GC, Case T-704/14, *Marine Harvest ASA v European Commission*, paras. 370-371. See too GC, Case T-609/19, *Canon v European Commission*, para. 461.

¹²³ See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, paras. 183-201.

¹²⁴ See correspondence attached to Complaint No 4.

behandlingsansvarlig har en «berettiget interesse» som overstiger den registrertes krav på personvern.

Vårt behandlingsgrunnlag er i hovedsak kontrakt, og i noen tilfeller samtykke. Ved oppstart av behandling av dine personopplysninger vil vi alltid gi informasjon om behandlingsgrunnlag.¹²⁵

Therefore, the privacy policy simply stated that SATS' legal basis for processing the personal data of its customers was generally “performance of a contract” and in some cases “consent”, but without specifying which purposes were covered by each of these legal bases.

However, Section 5.2 of SATS' general terms and conditions in effect in 2021 stated:

“Medlemmet samtykker til at SATS, og andre firmaer som inngår i samme konsern, registrerer, lagrer og bruker opplysninger om Medlemmet [...] Medlemmet samtykker til at SATS lagrer treningshistorikk med det formål å kunne følge opp Medlemmets aktivitet og tilrettelegge Medlemmets treningsopplegg”¹²⁶ (In the English version: “The Member consents to that SATS and other companies that are part of the same Group, registering, storing and using such personal data [...] The Member agrees that SATS can save training history data in order to be able to monitor Member activities and facilitate Member training”).¹²⁷

Moreover, Section 5.3 of SATS' general terms and conditions read:

“Medlemmet har rett til innsyn i sin treningshistorikk og kan kreve å få denne slettet. SATS skal bekrefte mottak av melding om sletting.”¹²⁸ (In the English version: “The Member can withdraw consent to their training history and request that such be deleted. SATS will confirm receipt of notification in respect of deletion”).¹²⁹

This wording (“samtykker”/“consent”) in the general terms and conditions suggests that the processing of training history data to monitor member activities and facilitate member training is one of those processing activities for which SATS relied on “consent” as a legal basis.

However, during our inquiry, SATS took the view that the term “samtykker”/“consent” in the general terms and conditions should not be interpreted as “consent” for GDPR purposes, and that SATS' legal basis for processing training history data was Article 6(1)(b) GDPR.¹³⁰ Nonetheless, in its written representations, SATS acknowledged that its communication regarding legal bases was imprecise.¹³¹

¹²⁵ See Personvernerklæring og informasjonskapsler – SATS (attached to Complaint No 4).

¹²⁶ Generelle vilkår for medlemskap i SATS – SATS (attached to Complaint No 4).

¹²⁷ SATS's General Terms and Conditions (English Version), applicable from 23.08.2021, available at <<https://www.sats.no/legal/english-version-of-our-general-terms-and-conditions>>.

¹²⁸ Generelle vilkår for medlemskap i SATS – SATS (attached to Complaint No 4).

¹²⁹ SATS's General Terms and Conditions (English Version), applicable from 23.08.2021, available at <<https://www.sats.no/legal/english-version-of-our-general-terms-and-conditions>>.

¹³⁰ See SATS' letter to Datatilsynet dated 28 April 2022.

¹³¹ See SATS' letter to Datatilsynet dated 31 October 2022, p. 5.

In addition, in its written representations, SATS claimed that it is up to the controller to determine the relevant legal basis, and that Datatilsynet is not in the position to challenge the controller's choice regarding the legal basis, as long as the latter is reasonable and justified.¹³²

Datatilsynet takes note of these arguments, but find them unconvincing. Although it is the controller's responsibility to ensure that it relies on a valid legal basis,¹³³ the validity of the legal basis chosen by the controller (and hence the lawfulness of the processing) may be verified and challenged by supervisory authorities,¹³⁴ as well as by data subjects.¹³⁵ Thus, it is not the case that Datatilsynet is not in the position to challenge the validity of the legal basis chosen by SATS. Moreover, the legal basis must be identified and communicated to data subjects at the outset of the processing;¹³⁶ it is not possible for the controller to "fix" the legal basis *ex post*. Therefore, the supervisory authority's assessment of the lawfulness of the processing should inevitably focus on the choice made by the controller at the outset of the processing, which should be assessed *inter alia* on the basis of the information that the controller has provided to data subjects.

With respect to the processing of training history data, SATS' general terms and conditions in effect in 2021 provides that SATS members "samtykker"/"consent" to the processing of such data. That wording is included in a section of the general terms and conditions with the heading "personopplysning, markedsføring og kommunikasjon", which exclusively deals with data protection and privacy matters. Thus, it seems illogical that the terms used in that section should not be interpreted in accordance with their standard meaning under data protection law, as SATS argued. Moreover, the English version of that section expressly states that consent can be withdrawn,¹³⁷ which further confirms that the section uses the term "consent" in accordance with the GDPR.¹³⁸ Finally, the fact that consent to the processing of training history data can be withdrawn under SATS' general terms and conditions confirms that such processing is not necessary for the performance of the membership contract, as outlined further below.

It should be noted that for consent to be valid under the GDPR it should generally be separate.¹³⁹ In this regard, the EDPB has opined that "the situation of 'bundling' consent with acceptance

¹³² See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating in Norwegian: "GDPR legger opp til at det er den behandlingsansvarlige som fastsetter sine behandlingsgrunnlag. Tilsynet kan neppe overprøve slike vurderinger så lenge de er forsvarlige og rimelige").

¹³³ See Arts. 5(1)(a) and (2), 6 and 24 GDPR.

¹³⁴ See Art. 57(1)(a) GDPR. See too e.g. CJEU, Case C-245/20, *X, Z v Autoriteit Persoonsgegevens*, para. 22 (assuming that supervisory authorities are generally competent to "review the lawfulness" of a processing operation, barring when the latter is carried out by a court in its judicial capacity).

¹³⁵ See Recital 63 GDPR (stating: "A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing" (emphasis added)).

¹³⁶ See EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para. 17.

¹³⁷ SATS's General Terms and Conditions (English Version), applicable from 23.08.2021, Section 5.3 (stating: "The Member can withdraw consent to their training history and request that such be deleted").

¹³⁸ See Article 7(3) GDPR.

¹³⁹ See Article 7(4) and Recital 43 GDPR. See further Case C-673/17, *Planet49* (Advocate General Opinion), para. 66.

of terms or conditions, or ‘tying’ the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of that contract or service, is considered highly undesirable. If consent is given in this situation, it is presumed to be not freely given”.¹⁴⁰

Therefore, the consent to the processing of training history data set out in Section 5.2 and tied to the acceptance of SATS’ general terms and conditions is invalid, as – contrary to what SATS argued¹⁴¹ – such processing is not invariably and objectively necessary to perform the contract.¹⁴² This is first and foremost evidenced by the fact that, as outlined above, SATS’ general terms and conditions allow members to withdraw their consent to the processing of the training history data and request that such data be deleted. In this regard, it should be noted that the general terms and conditions do not specify that any conditions apply to requests for deletion, they simply provide that SATS shall acknowledge receipt of such requests. Moreover, SATS’ processing of training history data is not objectively necessary to provide its services, at least to those members who intend to make only a basic use of SATS’ training facilities (e.g., without participating in group classes, without using a personal trainer, etc.), as access to SATS’ facilities to simply work out on one’s own does not require the recording of training history data. Furthermore, in its written representations, SATS stated that the processing of such data is “relevant”¹⁴³ to offer its services, but it failed to explain or show how such processing would be “necessary” to perform the contract with its members.¹⁴⁴ In this respect, the EDPB has opined that:

“necessary for the performance of a contract with the data subject [...] must be interpreted strictly and does not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller. Also the fact that some processing is covered by a contract does not automatically mean that the processing is necessary for its performance. [...] Even if these processing activities are specifically mentioned in the small print of the contract, this fact alone does not make them ‘necessary’ for the performance of the contract.”¹⁴⁵

¹⁴⁰ EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Adopted on 4 May 2020, para. 26.

¹⁴¹ See SATS’ letter to Datatilsynet dated 28 April 2022 (stating (in Norwegian): “lagring om treningshistorikk er nødvendig for at SATS skal kunne tilby en integrert del av sin tjeneste, nemlig treningsoppfølging. SATS tilbyr segregerte medlemskap, f.eks. medlemskap forbeholdt ett senter, sentre i en region eller medlemskap på landsbasis. I tillegg tilbyr SATS en rekke tilleggstjenester, f.eks. gruppertimer, PT-timer et c. SATS må følgelig behandle opplysninger om treningshistorikk (dvs. besøk og økter) for å blant annet holde oversikt over at medlemmets tilgang kjøpte og gjennomført e gruppertimer, PT-timer etc.”).

¹⁴² See EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para. 27 (stating: “Where a controller seeks to establish that the processing is based on the performance of a contract with the data subject, it is important to assess what is objectively necessary to perform the contract”).

¹⁴³ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 5 (stating (in Norwegian): “SATS mener at behandling av treningshistorikk er relevant for å tilby medlemmene treningsoppfølging, som er en sentral del av SATS’ tjenester» (emphasis added).

¹⁴⁴ It should be emphasised that the controller is responsible to demonstrate compliance with the lawfulness principle. See Article 5(2) GDPR.

¹⁴⁵ See EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para. 28.

In its written representations, SATS claimed that the EDPB's strict interpretation of Article 6(1)(b) has no basis in the GDPR.¹⁴⁶ Datatilsynet takes note of this argument. However, it should be dismissed in light of the case law of the CJEU on the notion of 'necessity of processing personal data'. Indeed, the CJEU has repeatedly found that "[a]s regards the condition relating to the necessity of processing personal data, it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary" (emphasis added).¹⁴⁷

In light of the above, neither Article 6(1)(a) nor Article 6(1)(b) was a valid legal basis for SATS' processing of training history data in the circumstances at hand, as the consent to such processing was not "freely given" and "informed", as it was tied to the general acceptance of SATS' terms and conditions, and in any event the processing at hand was not objectively necessary to the performance of the membership contract. Therefore, SATS violated Articles 5(1)(a) (lawfulness principle) and 6(1) GDPR, as it failed to have a valid legal basis in place to engage in the processing of training history data.

The fact that SATS failed to have a valid legal basis in place is further evidenced by the fact that, in response to a query from Complainant No 4, SATS noted that the legal bases for processing and retaining training history data was "Article 6(1)(b) and (f)",¹⁴⁸ and the latter (i.e., Art. 6(1)(f)) was neither mentioned as a relevant legal basis in the privacy policy nor in the general terms and conditions. This shows that the applicable legal basis was unclear also to SATS' staff.

It should be pointed out in passing that the choice of an appropriate legal basis is not a mere "technicality" of very limited importance to data subjects, as suggested by SATS.¹⁴⁹ Rather, it is essential to ensure compliance with a core principle of the GDPR (i.e., the lawfulness principle), which is of key importance to data subjects, as evidenced by the fact that Complainant No 4 took issue with the legal bases that SATS communicated to them. In any event, it is for SATS to identify an appropriate legal basis, should it wish to process training history data in the future.¹⁵⁰

¹⁴⁶ See SATS' letter to Datatilsynet dated 31 October 2022, p. 5.

¹⁴⁷ CJEU, Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*, para. 30 (and case law cited therein).

¹⁴⁸ See SATS' email to Complainant No 4 dated 10 October 2021 (referring to "behandlingsgrunnlaget i artikkel 6 nr. 1 bokstav b) og f)" (attached to Complaint No 4).

¹⁴⁹ See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating (in Norwegian): "Under enhver omstendighet kan det ikke være tvilsomt at GDPR artikkel 6(1)(f), berettiget interesse, er et gyldig behandlingsgrunnlag for treningshistorikk. Uenighet om gråsonene mellom artikkel 6(1)(b) og 6(1)(f) er langt på vei en "teknikalitet" med svært begrenset betydning, om noen, for medlemmene.").

¹⁵⁰ In its written representations, SATS sought Datatilsynet's input on whether Article 6(1)(f) could be an appropriate legal basis to process training history data in the future. See SATS' letter to Datatilsynet dated 31 October 2022, p. 5 (stating (in Norwegian): "SATS er åpen for heller å basere behandlingen av treningshistorikk på artikkel 6(1)(f) dersom Datatilsynet skulle mene at dette grunnlaget er mer treffende").

In its written submissions, SATS argued that Datatilsynet's conclusion that SATS breached Articles 5(1)(a) and 6(1) GDPR would violate the principle of *ne bis in idem*.¹⁵¹ Moreover, SATS argued that "it will always be the case that a breach of a specific obligation [in the GDPR] also represents a breach of one of the privacy principles"¹⁵² and therefore the two breaches should not be cumulated.¹⁵³ In this respect, it is sufficient to restate what has been mentioned above with respect to the other violations of Article 5: there is nothing in the GDPR that precludes a controller from being penalized both for an infringement of a principle in Article 5 and an infringement of the obligations stemming from that principle in the rest of the Regulation.¹⁵⁴ In the present case, by failing to have a valid legal basis for the processing of training history data, SATS has not only failed to make sure that "personal data [are] processed lawfully", as required by Article 5(1)(a); it also failed to make sure that one of the legal bases listed in Article 6(1) could validly be invoked.

7. Choice of Corrective Measure

Under Article 58(2) GDPR, Datatilsynet has several corrective powers, including the power to impose administrative fines for violations of the GDPR.

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, due regard must be given to the factors listed in Article 83(2)(a) to (k) GDPR. The following sub-sections outline how Datatilsynet has given "due regard" to these factors in the present case.

7.1. Nature, Duration and Gravity of the Infringements (Art. 83(2)(a))

As regards the criterion at Article 83(2)(a), SATS' infringements consist in having failed to comply with requirements whose violations may all be sanctioned in accordance with the higher tier of sanctions (Article 83(5)) under the GDPR's two-tier sanctions' system. In this regard, it should be noted that the GDPR "in setting up two different maximum amounts of administrative fine (10/20 million Euros), already indicates that a breach of some provisions of the Regulation may be more serious than for other provisions".¹⁵⁵ This only speaks to the intrinsic nature of some infringements (i.e., the infringements that may be fined up to 20 million Euros are—according to the assessment made by the legislator—by "nature" more serious than those that may be fined up to 10 million Euros). However, the actual gravity of a specific infringement should be assessed having regard also to other elements;¹⁵⁶ whether a violation is subject to a

¹⁵¹ See SATS' letter to Datatilsynet dated 31 October 2022, p. 9.

¹⁵² Ibid. (stating (in Norwegian): "Det vil så å si alltid være slik at et brudd på en konkret forpliktelse også representerer brudd på et av personvernprinsippene").

¹⁵³ Ibid.

¹⁵⁴ See EDPB, Binding decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, Adopted on 28 July 2021, paras. 183-201.

¹⁵⁵ Article 29 Data Protection Working Party, 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. 9.

¹⁵⁶ It should be noted that "nature" and "gravity" are two different and separate elements in Article 83(2)(a) GDPR.

maximum fine of 20 or 10 million Euros is only a starting point for assessing its gravity.¹⁵⁷ With respect to the nature of SATS’ infringements, it should also be noted that the infringements at hand concern “rights and obligations [that] are at the core of the fundamental right to data protection”.¹⁵⁸ We consider that, overall, SATS’ infringements may be deemed to be moderately serious in nature in the present circumstances.

The duration of most of the infringements is considerable. The access request of Complainant No 1 has remained unanswered since 2018, and SATS never provided a copy of the personal data of Complainant No 2 in response to their request in February 2019, although these data were finally deleted on 4 November 2021. SATS replied to Complainant No 4 only a couple of weeks late. However, SATS deleted certain personal data of Complainant No 2 and of Complainant No 3 on 4 November 2021, respectively about one and nineteen months after the expiry of the relevant exclusion period when the deletion should have taken place. As for the infringements of the lawfulness and transparency requirements, these are partially ongoing and have lasted at least since August 2021 (i.e., since the last update to the general terms and conditions). Such a – on the whole – prolonged state of noncompliance is one of the key elements to be taken into consideration in the analysis of the gravity of the infringements.

The gravity of the infringements should be assessed bearing in mind that they relate to rights and obligations that are at the core of the fundamental right to data protection. However, the impact of the infringements for the affected individuals, or at least for the complainants, appears to have been relatively modest in practice, as Datatilsynet has not been made aware of any specific damages suffered by the data subjects, apart from the emotional distress incurred, although the excessive retention of data on alleged wrongdoing could have had significant consequences for the relevant data subjects (e.g., a prolonged exclusion from the fitness centers). While the former element attenuates to a certain extent the gravity of the infringements, a central element of the analysis of their gravity should be whether the nature and scope of the infringements are indicative of broader, more systemic issues. In this regard, Datatilsynet considers that a multinational company, like SATS, should have sufficient policies, procedures and routines in place to enable the company to promptly and adequately respond to data subjects’ requests, and to meet the relevant storage limitation, transparency and lawfulness requirements.

In its written representations, SATS claimed that the identified infringements are not indicative of more systemic issues, as the present case concerns only a very small number of complaints.¹⁵⁹ However, in our view, the reoccurrence over a long period of time of several similar failures to ensure compliance with key data protection rights and obligations reveals that the infringements were not the result of occasional oversights. Instead, they are indicative of a failure to put in

¹⁵⁷ This is noted in response to SATS’ remark that the seriousness of a violation may not be assessed only on the basis of whether it may be sanctioned under Article 83(4) or (5). Cf. SATS’ letter to Datatilsynet dated 31 October 2022.

¹⁵⁸ EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, Version 2.0, Adopted on 13 October 2021, para. 2 (stating: “Data protection cannot be ensured without adhering to the rights and principles set out in the GDPR (Articles 12 to 22 [...], as well as Article 5 in so far as its provisions correspond to the rights and obligations provided in Articles 12 to 22 GDPR). All these rights and obligations are at the core of the fundamental right to data protection”).

¹⁵⁹ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 6.

place and follow adequate policies, procedures and routines. Moreover, through the assessment of the four complaints at issue in the present case, Datatilsynet has identified compliance issues that go beyond the mishandling of a few data subjects' requests (e.g., a failure to have a valid lawful basis in place for the processing of training history data in general, deficiencies in policies and documents that apply or applied to all of SATS' members, etc.). This is a systemic issue that enhances the gravity of the infringements. In this regard, it should be noted that most of the complaints concern data subjects' requests and policies that predate the Covid-19 pandemic. Thus, the pandemic should not be factored in when assessing the gravity of the infringements.

In respect of the number of affected data subjects, most of the violations affected four individuals in Norway (i.e., the complainants). However, some violations (i.e., the infringement of the transparency and lawfulness obligations) have affected virtually all of the about 700 000 SATS members.

Having considered the above, and taking into account all of the aforementioned aggravating and mitigating elements in their complexity, Datatilsynet considers the infringements to be moderately grave. This factor should be weighed accordingly in the present case.

7.2. Intentional or Negligent Character of the Infringements (Art. 83(2)(b))

In respect of the criterion at Article 83(2)(b), the EDPB found that:

*"In general, "intent" includes both knowledge and wilfulness in relation to the characteristics of an offence, whereas "unintentional" means that there was no intention to cause the infringement although the controller/processor breached the duty of care which is required in the law."*¹⁶⁰

Further to our inquiry, we see no evidence of an intentional infringement on the part of SATS. However, in our view, the infringements arose due to negligence on the part of SATS, insofar as the company failed to implement and follow appropriate measures to respond timely and properly to data subjects' requests, and to ensure – and be able to demonstrate – full compliance with storage limitation, lawfulness and transparency requirements, thus disregarding its duty of care.¹⁶¹ However, further to our inquiry, SATS seems to have taken some measures to improve its routines and state of compliance (see section 7.3 below).

It bears emphasizing that several staff members of SATS, including SATS' Customer Service Manager, have been involved in handling the above data subjects' requests, and that SATS' management is ultimately responsible for ensuring SATS' compliance with the GDPR. SATS has itself stated that the CEO has a responsibility for GDPR compliance.¹⁶² Therefore, it may

¹⁶⁰ Article 29 Data Protection Working Party, 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. These guidelines have been endorsed by the EDPB. See EDPB, Endorsement 1/2018 (adopted on 25 May 2018).

¹⁶¹ See Article 5(4) and 24 GDPR.

¹⁶² Generelle vilkår for medlemskap i SATS – SATS (attached to Complaint No 4) (stating: "Databehandlingsansvarlig for opplysningsene er SATS v/CEO.").

be concluded that several staff members of SATS have acted negligently in connection with the establishment and implementation of adequate compliance measures, as they disregarded their duty of care to ensure compliance with several legal obligations under the GDPR.¹⁶³

Overall, this factor should be weighed moderately against SATS in the present case.

In its written representations, SATS claimed that the negligence identified by Datatilsynet should be weighed neither against nor in favor of SATS. Datatilsynet disagrees with this view, and considers that the identified negligence should be weighed against SATS, albeit moderately. This is because SATS acted negligently over a prolonged period of time, despite the fact that several data subjects prompted SATS to bring its processing into compliance. Thus, the infringements are not due to a minor negligence, which occurred over a limited period of time. As a result, this degree of negligence should be given some weight for fining purposes. In this respect, the EDPB noted that “[d]epending on the circumstances of the case, the supervisory authority may also attach weight to the degree of negligence. At best, negligence could be regarded as neutral” (emphasis added).¹⁶⁴

7.3. Action Taken by the Controller to Mitigate the Damage Suffered by Data Subjects (Art. 83(2)(c))

SATS has taken several remedial actions, at least with respect to most of the infringements.¹⁶⁵ For example, after Datatilsynet’s inquiry, SATS has deleted the personal data of Complainant No 2, Complainant No 3 and Complainant No 4.¹⁶⁶ SATS has also updated its internal routines with the aim of ensuring a timelier handling of data subjects’ requests.¹⁶⁷ Further, SATS noted that it will consider amending Section 5.2 of its general terms and conditions.¹⁶⁸ All in all, this goes to the credit of SATS and should be weighed in favor of the company in the present case.

7.4. Degree of responsibility of the controller taking into account technical and organisational measures implemented pursuant to Articles 25 and 32 GDPR (Art. 83(2)(d))

The criterion at Article 83(2)(d) is not applicable in the present case, as the infringements contested in the case at hand do not concern technical and organisational measures implemented pursuant to Articles 25 and 32 GDPR.

¹⁶³ See HR-2021-797-A, and Section 46 of the Public Administration Act ('forvaltningsloven').

¹⁶⁴ EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0, Adopted on 12 May 2022, para. 57.

¹⁶⁵ However, some instances of non-compliance are yet to be remedied, for instance by responding to the access request of Complainant No 1, and by updating the privacy policy and general terms of service.

¹⁶⁶ See SATS’ letter to Datatilsynet dated 28 April 2022.

¹⁶⁷ Ibid.

¹⁶⁸ Ibid.

7.5. Relevant Previous Infringements by the Controller (Art. 83(2)(e))

The criterion at Article 83(2)(e) is not applicable in the present case, as SATS has not been sanctioned for similar or otherwise “relevant” infringements in the past.

In its written representations, SATS argued that the absence of previous infringements should be considered a mitigating factor.¹⁶⁹ This argument should be rejected. In this regard, it suffices to note that, under EU/EEA law, it is well established that the absence of any previous infringement is a normal circumstance, which should not be taken into account as a mitigating factor.¹⁷⁰ Moreover, the EDPB has specifically noted that “[t]he absence of any previous infringements, [...] cannot be considered a mitigating factor, as compliance with the GDPR is the norm. If there are no previous infringements, this factor can be regarded as neutral.”¹⁷¹

7.6. Degree of Cooperation with the Supervisory Authority (Art. 83(2)(f))

SATS has responded to Datatilsynet’s requests for information,¹⁷² although it demanded several deadline extensions,¹⁷³ and SATS’ cooperation did not go beyond what was required by law. Thus, in our view, this factor should be weighed neither in favor nor against SATS. As noted by the EDPB with respect to Article 83(2)(f) GDPR: “it would not be appropriate to give additional regard to cooperation that is already required by law”.¹⁷⁴ This was not disputed by SATS in its written representations.¹⁷⁵

7.7. Categories of Personal Data Affected by the Infringements (Art. 83(2)(g))

In light of the circumstances of the present case, the infringements committed by SATS do not appear to affect any special categories of personal data (within the meaning of Article 9 GDPR). However, some of them did affect information subject to a greater degree of sensitivity on the part of the individuals affected, such as data on their alleged wrongdoing. This element should be weighed moderately against SATS in the present case.

In its written representations, SATS argued that the factor in Article 83(2)(g) GDPR should be weighed in its favor.¹⁷⁶ The company claimed that the present case only affects “trivial data”, and that the information on “alleged wrongdoing” was deleted in accordance with SATS’

¹⁶⁹ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 7.

¹⁷⁰ See e.g. Joined Cases T-305/94, T-306/94, T-307/94, T-313/94, T-314/94, T-315/94, T-316/94, T-318/94, T-325/94, T-328/94, T-329/94 and T-335/94, *LVM v Commission*, para. 1163; Case T-8/89, *DSM v Commission*, para. 317.

¹⁷¹ EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, Version 1.0, Adopted on 12 May 2022, para. 94.

¹⁷² See the Factual Background above.

¹⁷³ See email from SATS’ Nordic Head of Legal & Compliance to Datatilsynet dated 27 October 2021; email from Brækhus Advokatfirma to Datatilsynet dated 31 March 2022; email from Brækhus Advokatfirma to Datatilsynet dated 19 April 2022; email from Advokatfirmaet Wiersholm to Datatilsynet dated 28 September 2022.

¹⁷⁴ Article 29 Data Protection Working Party, 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. 14.

¹⁷⁵ Cf. SATS’ letter to Datatilsynet dated 31 October 2022.

¹⁷⁶ Ibid, p. 7.

internal routines, and was thus not affected by the infringements identified by Datatilsynet.¹⁷⁷ This argument should be rejected. In this respect, it suffices to note that SATS kept its correspondence from 2019 with Complainant No 2 and Complainant No 3—which includes detailed information on their alleged misbehavior that led to their temporary ban from SATS’ gyms—at least until 2021.¹⁷⁸ This is despite the fact that, as outlined above, SATS’ retention policy provides that “If the customer relationship is terminated due to improper behavior from the member, name, date of birth and picture shall be kept for 60 months. Further, the member in question shall be marked as ‘excluded’. The rest of the data shall be deleted, included possible reports on the behavior” (emphasis added).¹⁷⁹ Therefore, contrary to what SATS argued in its written representations, the information on “alleged wrongdoing” was not deleted in accordance with SATS’ routines and is thus affected by the relevant infringements identified by Datatilsynet.

7.8. Manner in Which the Infringements Became Known to the Supervisory Authority (Art. 83(2)(h))

SATS’ infringements in the present case became known to Datatilsynet as a result of several complaints submitted over a period of four years. This factor should be weighed against SATS.

In its written representations, SATS argued that this factor should not be weighed against SATS, as this would amount to a violation of the principle against self-incrimination.¹⁸⁰ Datatilsynet acknowledges that SATS was not required to report the infringements to us out of its own motion, and that the mere fact that a controller did not spontaneously report an infringement to Datatilsynet is not an aggravating factor. However, the negligent conduct of the controller before the relevant infringement(s) became known to the supervisory authority—which ultimately triggered the involvement of the authority in the case—“may also be considered by the supervisory authority to merit a more serious penalty”.¹⁸¹ In this case, the infringements were brought to the attention of Datatilsynet by several data subjects, after and due to the fact that SATS failed to remedy the identified instances of non-compliance, despite the fact that these data subjects have previously attempted to prompt SATS to comply. Thus, the infringements were brought to the attention of Datatilsynet as a result of SATS’ failure to properly address the legitimate claims that various data subjects brought to its attention over the course of four years. This is the element that should be weighed against SATS in this case, and not the fact that it did not report the infringements to Datatilsynet of its own motion.

¹⁷⁷ Ibid.

¹⁷⁸ Excerpts from this correspondence were included by SATS in its replies to Datatilsynet dated 1 December 2021.

¹⁷⁹ In its correspondence with Complainant No 3 SATS also stated that such “rest of the data” would be deleted within 30 days. See email from kundeservice@sats.no to Complainant No 3 dated 11 October 2019 (attached to SATS’ letter to Datatilsynet dated 1 December 2021).

¹⁸⁰ See SATS’s letter to Datatilsynet dated 31 October 2022, p. 7.

¹⁸¹ See Article 29 Data Protection Working Party, 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.

7.9. Compliance with Corrective Measures Previously Ordered Against the Controller with Regard to the Same Subject-Matter (Art. 83(2)(i))

The criterion at Article 83(2)(i) is not applicable in this case, as no measures referred to in Article 58(2) GDPR have previously been ordered against SATS by Datatilsynet.

In its written representations, SATS argued that this factor should be weighted in favor of the company.¹⁸² This argument should be rejected. First, the wording of Article 83(2)(i) GDPR makes clear that this factor applies only “where measures referred to in Article 58(2) have previously been ordered against the controller”,¹⁸³ and no such measures have been ordered against SATS in the past. Secondly, the use of corrective measures is typically linked to the identification of an infringement and, as noted above (see Section 7.5), the absence of previous infringements—and hence of previous corrective measures—is a normal circumstance, which should not be taken into account as a mitigating factor.

7.10. Adherence to Approved Codes of Conduct or Certification Mechanisms (Art. 83(2)(j))

The criterion at Article 83(2)(j) is not applicable in this case, as SATS does not appear to adhere to any approved codes of conduct pursuant to Article 40 GDPR or approved certification mechanisms pursuant to Article 42 GDPR.

7.11. Any Other Aggravating or Mitigating Factor (Art. 83(2)(k))

Datatilsynet has not identified any other aggravating or mitigating factors in the present case. In this regard, it should be noted that, as outlined above, most of the complaints concern data subjects’ requests and policies that predate the Covid-19 pandemic. Thus, the latter does not appear to have had any significant impact on the infringements. Moreover, the reduction of SATS’ turnover due to the Covid-19 pandemic should not be considered a mitigating factor under Article 83(2)(k) GDPR.¹⁸⁴ This should be weighed neither against nor in favor of SATS in the present case.

In its written representations, SATS argued that some of the infringements concern facts that occurred in 2018 and 2019, shortly after the entry into force of the GDPR, and that this element should be weighed in SATS’ favor.¹⁸⁵ We find this argument untenable. It suffices to reiterate that: (1) SATS has not responded to the access request of Complainant No 1 to this date, and it deleted the data of Complainants No 2 and No 3 only after the opening of Datatilsynet’s inquiry in 2021, with the result that most of the violations identified by Datatilsynet were still ongoing in 2021; and (2) Datatilsynet’s assessment of the lawfulness and transparency of SATS’ processing has primarily focused on documents and policies that were still applicable in 2021 when we opened our inquiry. Furthermore, there were approximately two years between the

¹⁸² See SATS’ letter to Datatilsynet dated 31 October 2022, p. 8.

¹⁸³ See Article 83(2)(i) GDPR.

¹⁸⁴ EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 72.

¹⁸⁵ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 8.

entry into force of the GDPR in 2016¹⁸⁶ and the moment in which it started to apply in 2018.¹⁸⁷ Therefore, companies had at least two years to adapt to the new rules, and European supervisory authorities have repeatedly stated that there would be no “grace period” after the GDPR became applicable in 2018.¹⁸⁸

Moreover, SATS argued that the length of the administrative proceedings is a factor that Datatilsynet should consider under Article 83(2)(k) GDPR, in particular to reduce the amount of the fine. In support of this argument, SATS noted that one of the complaints was submitted to Datatilsynet in 2018, and referred to several cases in which the Norwegian Privacy Appeals Board (“Personvernemda”) reduced a fine imposed by Datatilsynet due to an excessive duration of the case handling which—according to Personvernemda—resulted in a violation of Article 6(1) of the European Convention on Human rights (ECHR).¹⁸⁹ In Datatilsynet’s view, this argument should be rejected for the following reasons.

First, Personvernemda has made clear that the duration of the administrative proceedings concerning the handling of a complaint should be calculated from the first request for information that Datatilsynet sent to the relevant controller,¹⁹⁰ and not from the moment Datatilsynet received the complaint.¹⁹¹ This appears to be meant to follow the case law on the reasonable duration of criminal proceedings of the European Court of Human Rights (“ECtHR”), which found that the starting-point of the period to be taken into consideration is when the person affected by the investigation became aware of the charges against them or when they were substantially affected by the measures taken in the context of the investigation or proceedings.¹⁹² In the present case, it is apparent that Datatilsynet first sent a request for information about Complaint No 1 to SATS on 23 March 2022¹⁹³ and notified SATS of its intention to issue an administrative fine on 26 September 2022. In other words, approximately six months elapsed before Datatilsynet notified SATS of its intention to issue an administrative fine. As for Complaints No 2, No 3 and No 4, it took Datatilsynet respectively approximately 1 year,¹⁹⁴ 11 months¹⁹⁵ and 6 months to notify SATS of its intention to impose an administrative

¹⁸⁶ See Art. 99(1) GDPR.

¹⁸⁷ See Art. 99(2) GDPR and § 32 personopplysningsloven.

¹⁸⁸ See e.g.: <<https://www.theparliamentmagazine.eu/news/article/gdpr-no-period-of-grace-following-entry-into-force>>; <<https://www.natlawreview.com/article/happy-gdpr-day>>.

¹⁸⁹ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 8.

¹⁹⁰ See PVN-2021-03 (stating (in Norwegian): “Nemnda legger for sin vurdering til grunn at forberedelsene med sikte på å avgjøre denne saken startet med tilsynets krav om redegjørelse”).

¹⁹¹ It should be stressed that the filing of a complaint does not invariably and automatically lead to the opening of an investigation.

¹⁹² ECtHR, *Mamić v. Slovenia* (no. 2), App. No. 75778/01, judgment of 27 July 2006, paras. 23-24; ECtHR, *Liblik and Others v. Estonia*, App. Nos. 173/15 and 5 others, judgment of 28 May 2019, para. 94.

¹⁹³ See the Factual Background above.

¹⁹⁴ As noted in the Factual Background, the first request for information regarding Complaint No 2 was sent on 7 September 2021 and Datatilsynet notified its intention to issue an administrative fine against SATS on 26 September 2022.

¹⁹⁵ As noted in the Factual Background, the first request for information regarding Complaint No 3 was sent on 5 October 2021 and Datatilsynet notified its intention to issue an administrative fine against SATS on 26 September 2022.

fine.¹⁹⁶ Moreover, approximately four months elapsed between the date in which Datatilsynet notified SATS of its intention to issue an administrative fine and the date of the final decision.¹⁹⁷ Thus, the duration of the administrative proceedings was overall shorter than that of those cases reviewed by Personvernemda—which SATS referred to in its written representations—which all lasted considerably more than one year.¹⁹⁸

Secondly, when determining whether the duration of the proceedings has been reasonable, due regard must be had to factors such as the complexity of the case, the applicant's conduct and the conduct of the relevant authorities.¹⁹⁹ With respect to the first factor, the present case is relatively complex, given that the violations contested to SATS concern several provisions of the GDPR, and several complaints were handled jointly. Moreover, the procedure set out in Articles 56(1) and 60 applies to the present case, which entails additional procedural steps (compared to the cases reviewed by Personvernemda and cited by SATS) and requires cooperation with foreign authorities. This adds to the complexity of the case.

As for the applicant's conduct, SATS contributed to the prolongation of the proceedings by asking for an extension of the procedural deadlines set by Datatilsynet essentially at each stage of the proceedings.²⁰⁰ In total, SATS has asked for—and has been granted—deadline extensions for a time period of approximately two months.

As for the conduct of the relevant authorities, Datatilsynet has made efforts aimed at higher procedural efficiency, for example by handling the complaints jointly in a single procedure, rather than opening several parallel inquiries. Moreover, it should be noted that Datatilsynet is currently confronted with an exceptional backlog of cases,²⁰¹ and the ECtHR has found that in similar circumstances some delays in the proceedings are not unjustified.²⁰² For instance, in *Buchholz v. Germany*, the ECtHR came to the conclusion that the duration of the proceedings was not unreasonable also because it found that it could not “overlook the fact that the delays [...] occurred at a time of transition marked by a significant increase in the volume of litigation”.²⁰³

Thirdly, it should be noted that the ECtHR has almost never found that proceedings lasting less than two years violated Article 6(1) ECHR due to their excessive duration. In the overwhelming majority of cases where the Court found a violation of Article 6(1) the proceedings had lasted

¹⁹⁶ As noted in the Factual Background, the first request for information regarding Complaint No 4 was sent on 23 March 2022 and Datatilsynet notified its intention to issue an administrative fine against SATS on 26 September 2022.

¹⁹⁷ See Datatilsynet's letter to SATS dated 26 September 2022.

¹⁹⁸ Cf. PVN-2021-16; PVN-2021-03; PVN-2021-09.

¹⁹⁹ ECtHR, *Liblik and Others v. Estonia*, App. Nos. 173/15 and 5 others, judgment of 28 May 2019, para. 91.

²⁰⁰ See email from SATS' Nordic Head of Legal & Compliance to Datatilsynet dated 27 October 2021; email from Brækhus Advokatfirma to Datatilsynet dated 31 March 2022; email from Brækhus Advokatfirma to Datatilsynet dated 19 April 2022; email from Advokatfirmaet Wiersholm to Datatilsynet dated 28 September 2022.

²⁰¹ The number of cases to be handled by Datatilsynet has been growing exponentially since 2018. Cf. Datatilsynet's Annual Reports <<https://www.datatilsynet.no/om-datatilsynet/arsmeldinger/>>.

²⁰² ECtHR, *Buchholz v. Germany*, judgment of 6 May 1981; ECtHR, *Zimmermann and Steiner v. Switzerland*, judgment of 13 July 1983; ECtHR, *Foti and others v. Italy*, judgment of 10 December 1982.

²⁰³ ECtHR, *Buchholz v. Germany*, judgment of 6 May 1981, para. 63.

four/five years or more.²⁰⁴ This is further supported by legal literature on the ECHR case law on this subject matter, which notes how “a total duration of up to 2 years per level of jurisdiction in non-complex cases is generally regarded as reasonable”.²⁰⁵ For example, an investigation which lasted one year and eight months was not considered unreasonably long.²⁰⁶

Having regard to the above, the duration of the proceedings against SATS has not been unreasonable.

7.12. Conclusion with Regard to Whether to Impose an Administrative Fine

Having had due regard to the factors under Article 83(2), the infringements that have been identified warrant the imposition of an administrative fine in the circumstances of this case.

Despite the relative limited number of individuals affected by some of the infringements (i.e., the infringements connected to the rights of access and erasure) and the remedial actions taken by SATS, the reoccurrence of similar instances of non-compliance over an extensive period of time and SATS’ approach towards the interpretation of its storage limitation, transparency and lawfulness obligations under the GDPR are indicative of systemic compliance flaws within the company, which—if not remedied—could result in important consequences for data subjects. In Datatilsynet’s view, the imposition of an administrative fine is therefore warranted to produce a genuine deterrent effect, and dissuade SATS—as well as companies in general—from committing similar infringements in the future. Indeed, enforcement efforts must generate sufficient pressure to make non-compliance economically unattractive in practice.²⁰⁷ This is particularly salient with regard to the kinds of infringements contested in the present case, as most of the administrative fines issued so far by European supervisory authorities concern the principles relating to processing of personal data; lawfulness of processing; valid consent; and transparency and rights of the data subjects.²⁰⁸

In its written representations, SATS claimed that the imposition of an administrative fine would be at odds with Datatilsynet’s administrative practice regarding corrective measures, and hence with the principle of equal treatment. SATS claims that the imposition of a reprimand would be a more suitable measure in the present circumstances. In this respect, SATS referred to a prior case in which Datatilsynet imposed a reprimand against a company that failed to comply with some of its transparency obligations under the GDPR.²⁰⁹ The latter case is, however, not

²⁰⁴ Cf. European Commission for the Efficiency of Justice (CEPEJ), Length of court proceedings in the member states of the Council of Europe based on the case law of the European Court of Human Rights (Council of Europe, 2018), pp. 112-122 <<https://rm.coe.int/cepej-2018-26-en-rapport-calvez-regis-en-length-of-court-proceedings-e/16808ffc7b>>.

²⁰⁵ See Henzelin and Rordorf, ‘When Does the Length of Criminal Proceedings Become Unreasonable According to the European Court of Human Rights?’ 5(1) (2014) *New Journal of European Criminal Law* 79-109, p. 93.

²⁰⁶ ECtHR, *Idalov v. Russia*, App. No. 5826/03, judgment of 22 May 2012, paras. 190-191.

²⁰⁷ See Opinion of Advocate General Geelhoed in Case C-304/02, *Commission v. France*, delivered on 29 April 2004, para. 39.

²⁰⁸ EDPB, Contribution of the EDPB to the evaluation of the GDPR under Article 97, Adopted on 18 February 2020, pp. 33-34.

²⁰⁹ See SATS’ letter to Datatilsynet dated 31 October 2022, p. 9 (referring to Reprimand and Compliance Order - Mowi ASA, Doc. No 21/03656-12).

comparable with the present one, as it concerns only: (1) a failure to respond to a single access request on time due to the fact that such request ended up in the spam folder of the company’s email inbox, a matter that was eventually amicably settled; and (2) a delayed provision of all of the information in Article 14 GDPR (which—contrary to Article 13—does not require that information be provided at the time of the processing, but within a month), which was eventually considered satisfactory by the relevant complainant.

At present, Datatilsynet has not handled other cases which may be deemed largely comparable to the present one. However, it should be emphasised that Datatilsynet has issued fines against other controllers too, including in circumstances where they had violated only some of the legal requirements violated by SATS and where such violations affected a single data subject.²¹⁰

7.13. Calculation of the Amount of the Administrative Fine

Having had due regard to the factors under Article 83(1) and (2), we find an administrative fine of NOK 10 000 000 (ten million) to be appropriate in the circumstances of this case. This is for the reasons outlined below. In this respect, it should be noted that the setting of a fine is not an arithmetically precise exercise,²¹¹ and supervisory authorities have a certain margin of discretion in this respect.²¹² Nonetheless, they should indicate the factors that influenced the exercise of their discretion when setting a fine.²¹³

In terms of the requirement under Article 83(1) to ensure that the imposition of the fine in the circumstances of this case is effective, proportionate and dissuasive, the financial position of SATS must be taken into account. The financial position of SATS is also relevant to determine the maximum fine applicable in the present case.

In 2021, SATS’ total annual turnover appears to be of NOK 3 247 million.²¹⁴ Thus, the maximum fine applicable in the present case is EUR 20 000 000 (i.e., around NOK 200 000 000), as the latter amount is higher than 4% of the company’s total annual turnover, and Article 83(5) provides that infringements of Articles 5, 6, 12, 15 and 17 GDPR shall 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” (emphasis added).

Having considered the above, a fine of NOK 10 000 000 (ten million) seems appropriate, as it represents approximately 5% of the maximum applicable fine and sits within the lower end of the spectrum of possible fines. Therefore, such a fine is commensurate with the seriousness of

²¹⁰ See e.g. Case 20/01874, Basaren Drift AS; Case 20/02220, Flisleggingsfirma AS; Case 20/02375, Ultra-Technology AS.

²¹¹ See, *inter alia*, Case T-425/18, *Altice Europe NV v Commission*, para. 362; Case T-11/06, *Romana Tabacchi v Commission*, para. 266.

²¹² See, *inter alia*, Case T-192/06, *Caffaro Srl v Commission*, para. 38.

²¹³ EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 75.

²¹⁴ See SATS Annual Report 2021, available at <<https://satsgroup.com/wp-content/uploads/2022/03/SATS-ASA-Annual-Report-2021.pdf>>.

the infringements for which it is imposed, taking into account all of the aggravating and mitigating factors outlined above (see sections 7.1-7.12 above).

Such a fine would represent approximately 0.3% of SATS' annual turnover for 2021. Therefore, it would have some significance to the company relative to its revenue—which is essential to ensure its dissuasive effect—without being disproportionate relative to the company's financial position and the infringements viewed as a whole.

The amount of the fine set out above takes into account that SATS' total annual turnover for 2021 decreased by 8% compared to 2020, primarily due to club closures and visit restrictions because of the Covid-19 pandemic.²¹⁵ While this is not a mitigating factor, Datatilsynet believes that the fine should be slightly adjusted in view of the difficult economic context in which the company is operating due to the pandemic.

For the sake of clarity, it should be noted that Datatilsynet has calculated the above fine on the basis of all of the infringements viewed as a whole, and has not cumulated separate fines for each of the individual infringements identified. In any event, given that all of the provisions violated by SATS may be fined up to 20 000 000 EUR, the total amount of the administrative fine has not exceed the amount specified for the gravest infringement, as demanded by Article 83(3) GDPR.

In its written representations, SATS claimed that the amount of the fine indicated above is disproportionately high and it would not be in line with the existing administrative practice across the EU/EEA regarding administrative fines.²¹⁶ In this respect, we reiterate that the setting of a fine is not an arithmetically precise exercise,²¹⁷ and supervisory authorities have a certain margin of discretion in this respect.²¹⁸ In any event, the cherry-picked selection of cases listed in SATS' written representations in support of its claim—none of which is entirely analogous to the present one—only focuses on the numeric value of the fines imposed, but does not show how each of the amounts relate to the economic size of the recipient of the fine.²¹⁹ The size of the undertaking concerned is one of the key elements that should be taken into account in the calculation of the amount of the fine in order to ensure its dissuasive nature.²²⁰ Taking into consideration the resources of the undertaking in question is indeed justified by the impact sought on the undertaking concerned, in order to ensure that the fine has sufficient deterrent

²¹⁵ Ibid.

²¹⁶ See SATS' letter to Datatilsynet dated 31 October 2022, p. 10.

²¹⁷ See, *inter alia*, Case T-425/18, *Altice Europe NV v Commission*, para. 362; Case T-11/06, *Romana Tabacchi v Commission*, para. 266. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 74.

²¹⁸ See, *inter alia*, Case T-192/06, *Caffaro Srl v Commission*, para. 38. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 74.

²¹⁹ Cf. SATS' letter to Datatilsynet dated 31 October 2022, p. 10.

²²⁰ EDPB, Decision 1/2021 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding WhatsApp Ireland under Article 65(1)(a) GDPR, paras. 405-412; EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 76.

effect, given that the fine must not be negligible in the light, particularly, of its financial capacity.²²¹

Having regard to the above, a fine equal to 0.3% of SATS' annual turnover for 2021 is in line with fines issued in partially similar cases, including cases reviewed by Personvernemda. In this respect, it suffices to note that in a case concerning violations of Articles 6(1) and 13 that Personvernemda did not consider too serious, Personvernemda deemed a fine equal to 0.9% of the annual turnover of the preceding financial year to be adequate.²²² Further, in a case concerning a serious violation of Article 6(1), Personvernemda considered a fine equal to 7.9% of the annual turnover of the preceding financial year to be "not too high".²²³ In this respect, it should be emphasized that SATS' infringements concern more provisions of the GDPR and affected more individuals compared to the latter two cases.

8. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, pursuant to Article 22(2) of the Norwegian Data Protection Act, the present decision may not be appealed before Personvernemda. However, the present decision may be challenged before Oslo District Court ("Oslo tingrett") in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act and Article 4-4(4) of the Norwegian Dispute Act.²²⁴

Kind regards

Line Coll
Data Protection Commissioner

Luca Tosoni
Specialist Director

This letter has electronic approval and is therefore not signed

Copy to: Complainants; ADVOKATFIRMAET WIERSHOLM AS

²²¹ Case C-408/12 P, *YKK and Others v Commission*, para 85; Case C-413/08 P, *Lafarge v European Commission*, para. 104 and the case law cited therein. See too EDPB, Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR, adopted on 15 June 2022, para. 76.

²²² See PVN-2021-13.

²²³ See PVN-2020-21.

²²⁴ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

Summary Final Decision Art 60 Complaint

EDPBI:NO:OSS:D:2023: 665

Violation identified ; Administrative fine

Background information

Date of final decision:	06 February 2023
Date of broadcast:	20 February 2023
LSA:	NO
CSAs:	FI, DK, SE.
Legal Reference(s):	Article 5 (Principles relating to processing of personal data) , Article 6 (Lawfulness of processing), 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')).
Decision:	Violation identified, Administrative fine.
Key words:	Lawfulness of processing, Transparency, Right to erasure, Right to rectification, Data subject rights.

Summary of the Decision

Origin of the case

The inquiry focused on the controller's compliance with Articles 5, 6, 12, 13, 15 and 17 GDPR in connection with the complaints against it lodged with the NO SA between 2 October 2018 and 8 December 2021. All such complaints concerned alleged infringements of data subjects' rights committed by the controller, in connection with its handling of data subjects' requests submitted pursuant to Articles 15 and 17 GDPR. In the **first complaint**, the complainant claimed that the controller had transferred the personal data to other companies within its corporate group, as well as to Facebook outside the EU/EEA, without a proper legal basis. The complainant claimed also that an access request submitted on 29 August 2018 pursuant to Article 15 GDPR had remained unanswered. In the **second complaint**, the complainant claimed that the controller had failed to respond to an access request submitted on 25 February 2019 pursuant to Article 15 GDPR and that it had refused to comply with an erasure request submitted on the same date pursuant to Article 17 GDPR, after the membership to the fitness centre run by the controller was terminated by the controller. In the **third complaint**, the complainant claimed that the controller had refused to comply with an erasure request submitted on 5 October 2019 pursuant to Article 17 GDPR, following the termination of the membership by the controller. In the **fourth complaint**, the complainant claimed that the controller

had refused to comply with an erasure request regarding their training history submitted on 6 August 2021 pursuant to Article 17 GDPR.

Findings

In the first place, the NO SA found that, by failing to timely act upon two separate access requests, the controller had infringed **Articles 12(3) and 15 GDPR**. The NO SA stated that the fact that other companies faced challenges with adapting to the GDPR after it became applicable in 2018 is not a valid justification for a violation of the GDPR that started to occur in September 2018.

In the second place, the NO SA found that, by failing to take prompt action and erase certain personal data without undue delay pursuant to three separate erasure requests, the controller had infringed **Articles 5(1)(e), 12(3) and 17 GDPR**. For two of the erasure requests, the original purpose of processing had been to enforce the exclusion of banned members. However, the controller retroactively stated that the purpose of the storage is to be able to process the information in connection with the ban and that this purpose does not expire as soon as the ban is lifted. It also claimed that such a change of position on the purpose would not affect the assessment of the legitimacy of the retention period. The NO SA emphasized that it is not possible to adjust the relevant purpose *ex post*; the assessment of retention should be made with respect to the purpose identified by the controller at the outset of the relevant processing. In the third erasure request, the complainant withdrew their consent to storage of their training history as the controller's terms and conditions stated that they were entitled to. The controller stated that the legal basis was not consent and that it could retain the personal data for a period of six months in light of the ongoing pandemic. The NO SA found that a storage period of six months was not justified and that in any case, the controller retained the personal data in question for longer than six months.

In the third place, the NO SA found that, by failing to duly inform data subjects about its data retention policy concerning the personal data of banned members and the relevant legal basis for the processing, the controller had infringed **Articles 5(1)(a), 12(1) and 13 GDPR**. The controller has established a specific data retention policy with respect to the personal data of members whose membership is terminated by the controller. Nonetheless, no publicly available documents provide specific information on the retention period at hand. In the view of the NO SA, the controller violated Articles 5(1)(a) and 13(2)(a) GDPR as it failed to ensure transparency about legal bases, the period for which it stores the personal data of banned members and/or the criteria used to determine that period. It is not sufficient to inform data subjects about the retention period when the controller notifies them of the termination of their membership.

Lastly, the NO SA found that, by failing to rely on a valid lawful basis to process the training history data of the members of its fitness centres, the controller had infringed **Articles 5(1)(a) and 6(1) GDPR**. The privacy policy simply stated that the controller's legal basis for processing the personal data of its customers was generally "performance of a contract" and in some cases "consent", but without specifying which purposes were covered by each of these legal bases. The terms and conditions stated that processing of training history was based on consent. The consent to the processing of training history data tied to the acceptance of the controller's general terms and conditions is invalid. Neither Article 6(1)(a) nor Article 6(1)(b) was a valid legal basis for the controller's processing of training history data as the consent to such processing was not "freely given" and "informed", as it was tied to the general acceptance of the controller's terms and conditions, and in any event the processing was not objectively necessary to the performance of the membership contract.

Decision

The NO SA found that the controller had infringed **Articles 5, 6, 12, 13, 15 and 17 GDPR** in handling the data subjects' requests submitted pursuant to Articles 15 and 17 GDPR.

Pursuant to Article 58(2)(i) GDPR, the NO SA issued an administrative fine of NOK 10 000 000 (ten million) against the controller.

[Complainants contact information]

Exempt from publicity:

The Freedom of Information Act

Section 13, cf. the Personal Data Act

Section 24 first paragraph, second sentence

Your reference

Our reference
20/02107-18

Date
02.03.2023

Closure of case – Transmotor ApS

Datatilsynet refers to your complaint of 6 May 2019 regarding the processing of your personal data by Transmotor ApS (Transmotor). We informed you in a letter of 21 January 2021 that this is a so-called cross-border case, which according to data protection rules is subject to different case handling rules than ordinary cases, see Article 4(23) and 56(1) GDPR. The case has been handled by the Data Protection Authority in Denmark as lead supervisory activity, since the company has its sole establishment in Denmark. The Norwegian and Swedish Data Protection Authorities have participated in the case as concerned supervisory authorities.

About the case handling

The Danish Data Protection Authority has investigated the case by contacting Transmotor. They also asked for your feedback to the company's response. They have cooperated with us and the Swedish Data Protection Authority to assess the case based on your complaint and other information you have given us, in addition to the response from the company. We have together with them made a decision. The case handling has followed the procedure in Article 60 of the GDPR, whereby the Data Protection Authority in Denmark presented a draft decision. We agree with the Danish Data Protection Authority's draft decision and we are therefore taking the final decision in line with their conclusions.

Our assessment

The Data Protection Authority closes the case with reference to the reasons in the decision that follows below. The decision is written in English, but we can assist with translation. If you want us to translate, please contact us.

Complaint about Transmotor ApS

1. The Danish Data Protection Agency (hereinafter referred to as the ‘Danish DPA’) hereby returns to the case, where you on 6 May 2019 have complained to the Norwegian Data Protection Authority about the processing of your personal data.

In accordance with Article 56 of the GDPR¹, the Danish DPA has been designated as the lead supervisory authority in the case. The Norwegian and Swedish DPAs have been involved as concerned supervisory authorities.

2. Facts of the case

The Danish DPA has understood your inquiry as a complaint regarding the Chief Executive Officer of Transmotor ApS’ (hereinafter “Transmotor”) access to your work e-mail for an undefined period of time, without your consent and without informing you of this access, while you were employed at Transmotor Norge AS.

According to the case facts, Transmotor Norge AS was a subsidiary to Transmotor ApS while you were employed. Subsequently, Transmotor Norge AS went bankrupt. It is the DPA’s understanding, that the Chief Executive Officer of Transmotor ApS acted as Chief Executive Officer of Transmotor AS as well.

Furthermore, you have stated that Transmotor disclosed personal data regarding your resignation to Transmotor’s customers, suppliers and collaborators.

In contrast, Transmotor has stated that the company informed you about Transmotor’s access to your work e-mail. Transmotor claims that the access to your e-mail has been in accordance with the Danish DPA’s guidelines and the principles for the processing of personal data in Article 5 of the GDPR. According to Transmotor, the company had a legitimate interest on the basis of Article 6(1)(f) of the GDPR in accessing relevant correspondence with suppliers and business partners and that the access to your e-mail has been used only for this operational purpose after termination of the employment. Furthermore, Transmotor has stated that Transmotor only kept the e-mail active for a period as short as possible after the termination of the employment considering your position and function, and that your e-mail has been deactivated subsequently.

Furthermore, Transmotor has stated, that Transmotor is not the data controller of the processing of personal data. In the view of Transmotor, the fact that Transmotor Norge AS was declared bankrupt does not mean that the Danish company succeeds in the controllership of Transmotor Norge AS.

On the 22th of June 2022, the Danish DPA requested you of a copy of the transmitted e-mail regarding your resignation. By e-mail of August 2 2022 you have stated, that you cannot find the e-mail in question.

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).

3. The Danish DPA's assessment

The Danish DPA has considered the information provided in the case, and on this basis conducted a brief investigation of the matter. Subsequently, The Danish DPA has concluded that the DPA will not take further action in connection with your inquiry of 6 May 2019. The case hence is concluded with this letter.

The reasons for the Danish DPA's conclusion are set out below.

Initially, the Danish DPA notes that there is conflicting information in the case with regards to whether Transmotor provided you with sufficient information regarding Transmotor's access to your work e-mail. You claim that you did not receive information hereof and Transmotor, on the other hand, stated that you were well aware and sufficiently informed. The Danish DPA notes, that the DPA is not able to carry out an actual evidence assessment when there is disagreement between the parties about the facts in the case as the Danish DPA handles cases on a written basis. The final assessment of such evidential issues should be determined by the police or the courts, which, unlike the Danish DPA, have the opportunity to clarify the facts, e.g. by questioning witnesses. The Danish DPA finds that there are no grounds for the DPA in the present case to file a police report.

Furthermore, in the Danish DPA's view, it is uncertain whether Transmotor ApS (and not Transmotor Norge AS) is to be considered the data controller for the processing of personal data in question, including sending the e-mail to Transmotor's customers, suppliers and collaborators.

Finally, in the opinion of the Danish DPA, your complaint only to a limited extent concerns data protection law, as the case mainly concerns issues of employment law due to an employment law dispute.

It is the Danish DPA's assessment, that a further examination and use of the Danish DPA's resources associated with such an examination is not commensurate with what could be achieved by doing so.

The Danish DPA refers to Article 57(1)(f) of the GDPR, which states that the DPA must deal with complaints lodged by a data subject and, where appropriate, investigate the subject matter of the complaint.

It follows from the said provision that the DPA decides whether it is appropriate to examine the subject matter of the complaint. In making this assessment, the DPA may, for example, consider the resources available to the DPA and the potential result expected to be achieved by an examination of the subject matter of the case. When the Danish DPA has concluded that it does not intend to initiate a further investigation of the matters, it is due to the fact that the Danish DPA has assessed what could potentially be achieved by initiating a further investigation of the case, including to what extent it could specifically improve your legal position, or whether such an investigation could in general be suitable for raising the level of data protection.

The Danish DPA hereby considers the case to be closed, after having obtained the approval of the concerned supervisory authorities, and will take no further action in connection with your inquiry.

Legal review of the decision

Since this is a cross-border case and a final decision has been made, it is not possible to file an administrative complaint against the decision. The Personal Data Act section 22 second paragraph, second sentence, states that decisions made through cooperation between the lead supervisory authority and other supervisory authorities concerned cannot be appealed to the Privacy Appeals Board.

You may challenge the decision before the courts if you are of the opinion that the decision is incorrect or invalid.

Best regards

Tobias Judin
Head of Section

Guro Fiskvik Åsbø
Senior legal advisor

This document is signed electronically and therefore includes no handwritten signatures



Datatilsynet

[REDACTED]

Exempt from public disclosure:

Offl § 13 jfr Popplyl. § 24

Your reference

Our reference

20/02425-8

Date

02.05.2023

Avslutning av sak - L'AMOURBOX ApS

Datatilsynet viser til din klage av 14. februar 2019 angående L'AMOURBOX ApS (sak 20/02425). Dette er en sak som måtte håndteres av datatilsynet i Danmark der virksomheten har hovedkontoret sitt, jf. personvernforordningen artikkel 4 nr. 23 og artikkel 56 nr. 1.

Om saksbehandling

Datatilsynet i Danmark har gjort undersøkelser i saken ved å ta kontakt med L'AMOURBOX ApS. Etterpå samarbeidet de med oss om å vurdere saken basert på klagen din og øvrig informasjon du har gitt oss, i tillegg til svaret fra virksomheten. Vi har i fellesskap fattet avgjørelse i saken, i henhold til personvernforordningen artikkel 60.

Avgjørelsen

Den felles avgjørelsen fra det norske og danske datatilsynet følger under. Avgjørelsen er skrevet på engelsk, men vi kan bistå med å oversettelse dersom det er ønskelig. I så fall ber vi deg om å ta kontakt.

Overprøving av vedtaket

Ettersom dette er en grenseoverskridende sak og en endelig beslutning er truffet, er det ikke mulig å klage på vedtaket etter forvaltningsloven. Det følger av personopplysningsloven § 22 annet ledd annet punktum at vedtak som utarbeides gjennom samarbeid mellom ledende tilsynsmyndighet og andre berørte tilsynsmyndigheter ikke kan påklages til Personvernministeriet. Du kan imidlertid bringe saken inn for domstolene dersom du mener at vedtaket er feil eller ugyldig.

Decision

The Norwegian Data Protection Authority, Datatilsynet (“Norwegian DPA”) refers to the complaint against L'AMOURBOX ApS you submitted on 14 February 2019 concerning the fact that, in February 2019, by accessing the chat function on www.lamourbox.no, you could access other customers' previous chat history with L'AMOURBOX, in which information about the customer's name, address and possible purchases appeared.

After having reviewed your complaint, the Norwegian DPA concluded that your complaint concerned a cross-border processing of personal data (within the meaning of Article 4(23) of the General Data Protection Regulation (GDPR)), which meant that the case had to be processed in cooperation with the supervisory authorities of other EU/EEA Member States in accordance with Article 60 GDPR.

In cases that concern a cross-border processing of personal data, the supervisory authority of the main establishment or of the single establishment of the relevant company – which in this case is located in Denmark – shall be competent to act as lead supervisory authority. Thus, in the present case, the Danish Data Protection Agency (“Danish DPA”) acted as lead supervisory authority.

While handling the case, the Danish DPA asked L'AMOURBOX on 9 August 2022 if other customers had unauthorized access to your personal data via the chat function on L'AMOURBOX's website.

The Danish DPA received an answer from L'AMOURBOX on 22 August 2022, which stated that a technical fault in its chat function allowed its customers to have unauthorized access to other people's chats for a short period of time. However, L'AMOURBOX has not confirmed that other customers had unauthorized access to your personal data via the chat function. The Danish DPA informed the Norwegian DPA about the inquiry on the same day.

After examining the case, the Danish DPA found that there were no grounds for the Danish DPA to take further action regarding the case. This was due to the fact that Section 39(1) of the Danish Data Protection Act states that a data subject can only lodge a complaint with a supervisory authority regarding processing of data relating to him or her. Conversely, a data subject cannot lodge a complaint with a supervisory authority regarding the processing of data that does not relate to him or her.

In light of the information provided by L'AMOURBOX's and the Danish DPA's inquiry in to the matter at hand, it may not be concluded that other customers had unauthorized access to your personal data, and thus that the processing described in your complaint relates to you. On this basis, your complaint shall be rejected.

The Norwegian DPA will take no further action regarding the case and considers it to be closed. However, it takes note of the information you provided in your complaint, which may be used for future investigative purposes.

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, the present decision may be appealed before Oslo District Court (“Oslo tingrett”) in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act, and Article 4-4(4) of the Norwegian Dispute Act.

Vennlig hilsen,

Tobias Judin
seksjonssjef

Luca Tosoni
juridisk fagdirektør

This letter has electronic approval and is therefore not signed

ADVISTA AS
Nydalsveien 36
0484 OSLO

Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven
§ 24 første ledd 2. punktum

Your reference

Our reference

22/00194-19

Date

05.06.2023

'Sui Generis' Decision - Advista AS

On 12 January 2022, the Spanish Agency for Data Protection (“Agencia Española de Protección de Datos”, “Spanish SA”) shared with the Norwegian Data Protection Authority (“Datatilsynet”, “us”, “our”) a complaint lodged by [REDACTED] (the “complainant”) against Advista AS (“Advista”). The latter is a Norwegian company that, in 2021, used to operate the website teloos.es.

The complainant argued that Advista failed to respond to an erasure request they submitted under Article 17 of the General Data Protection Regulation (“GDPR”). The request concerned the complainant’s name, surnames and postal address, which in 2021 were available on teloos.es.

Further to our inquiry, Advista informed us that the website teloos.es has since been closed and that the data it included have been deleted. Advista also told us that they have no record of having received an erasure request from the complainant. However, Advista claimed that it may be that such request was not received due to the fact that the process that led to the closure of the website started in 2021, and it is thus possible that the complainant submitted their request through a form or an email address that were no longer in use at the time of the request. In any event, the complainant’s personal data have been deleted as a result of the closure of the website teloos.es.

Taking into account that the closure of the website has essentially mooted the issues raised in the complaint and that supervisory authorities “should seek an amicable settlement with the controller”, on 24 February 2023, the Spanish SA wrote a letter to the complainant to inform them about the closure of the website teloos.es and to invite them to express any objections they may have against the closure of the present case. The letter also informed the complainant that if they will not respond to the letter within three weeks upon receiving it, we will consider that the matter has been resolved to the complainant’s satisfaction and we will close the present case.

In light of the above, and given that the complainant has not responded to the above-mentioned letter within the set deadline, we consider that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR, and that the matter may be deemed to be resolved to the complainant's satisfaction. We have therefore decided to close the present case in accordance with Article 60(7) GDPR and the requirements of Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021).

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

This letter has electronic approval and is therefore not signed

Copy to: Agencia Española de Protección de Datos



Your reference

Our reference

23/00909-11

Date

27.03.2024

Rejection of Complaint - DNB Bank ASA

1. Introduction

The Norwegian Data Protection Authority (hereinafter “Datatilsynet”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“GDPR”)¹ with respect to Norway.

[REDACTED] (hereinafter “complainant”) is a customer of DNB Bank ASA (hereinafter “DNB”, “bank” or “controller”) who suspects that one of the bank’s employees who carried out consultation operations on her bank account did not actually act under the authority and in accordance with the instructions of DNB. The complainant considers the information provided by the controller to be insufficient to enable her to dispel her doubts as to the lawfulness of the processing of her personal data, and lodged a complaint with Datatilsynet asking that we carry out an investigation to dispel her doubts.

After having requested DNB to provide us with the information we needed in order to examine the complaint, we have found no evidence that one of the bank’s employees carried out consultation operations on the complainant’s personal data against or beyond the instructions received from DNB.

In light of the above, we have decided that the complaint shall be rejected as unfounded.

2. Decision

Datatilsynet adopts the following decision on the complaint submitted by [REDACTED] against DNB (national case number 23/00909):

- The complaint shall be rejected as unfounded pursuant to Article 60(8) GDPR.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

3. Factual Background

In 2019, the complainant asked DNB to provide her with a report on the consultation operations carried out by the employees of the bank on her bank account.

On 25 March 2019, DNB sent the requested report to the complainant. The report indicated the dates and the number of consultation operations carried out on the complainant's bank account.

After having reviewed such a report, the complainant considered that the number of consultation operations was "not normal", and asked DNB to investigate whether there had been any unauthorized access to her personal data.

DNB carried out the requested internal investigation, and on 10 May 2019 it informed the complainant that it did not identify "anything illegal or suspicious" (in Norwegian, "det er ikke avdekket noe ureglementert eller mistenkelig").

The complainant considered the information provided by the controller to be insufficient to enable her to dispel her doubts as to the lawfulness of the processing of her personal data, and lodged a complaint with Datatilsynet asking that we carry out an investigation to dispel her doubts.²

On 26 January 2024, Datatilsynet wrote to the complainant to inform her that, after having reviewed the documentation she produced, Datatilsynet had not identified any elements to call the conclusion reached by DNB's internal investigation into question. Therefore, Datatilsynet intended to close the case.

On 26 January 2024, the complainant wrote to Datatilsynet to express her insistence that Datatilsynet should continue investigating this case. The complainant justified this request on the grounds that she suspected that a female friend of her mother, employed at the "DnB Linderud" office, had been accessing the complainant's bank account many times over the past several years on behalf of the complainant's mother.

On 31 January 2024, Datatilsynet wrote to the complainant to ask her to provide us with the name of the DNB's employee she suspected, and to explain on what grounds she suspected that the employee in question had carried out unauthorized accesses to her bank account. The complainant never responded to this request.

Datatilsynet also wrote to DNB to ask the controller to provide us with a list of employees who had carried out consultation operations on the complainant's bank account since 2019, as well as the dates and purposes of those operations. DNB provided Datatilsynet with such information on 12 February 2024.

² The first communication regarding this case was received by Datatilsynet on 8 March 2023. However, in that communication the complainant referred to a previous letter she sent to Datatilsynet, but which appears to have gone missing.

4. Legal Background

GDPR

Article 5(1)(a) GDPR provides that personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject.

Furthermore, Article 29 GDPR provides as follows:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

The GDPR also establishes the following data subjects' rights, which are relevant in the present case:

Pursuant to Article 12(3) 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. 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.

Pursuant to Article 15 GDPR:

- 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.

EEA and Norwegian Law

The GDPR has been incorporated into Annex XI to the European Economic Area (“EEA”) Agreement by means of Decision of the EEA Joint Committee No 154/2018 (“EEA Joint Committee Decision”).³

Article 1(b) of the EEA Joint Committee Decision provides that:

[...] the terms “Member State(s)” and “supervisory authorities” shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively.

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively.

The Norwegian Personal Data Act incorporated the GDPR into Norwegian law.⁴ The Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.

5. Datatilsynet’s Competence

In its letter to DNB of 29 January 2024, Datatilsynet asked DNB to confirm whether the processing at issue in the present case qualifies as “cross-border processing” within the meaning of Article 4(23) GDPR. In its response dated 12 February 2024, DNB confirmed this, and stated that DNB has an office in Latvia whose employees can access the bank’s customer database

³ Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

⁴ Act No 38 of 15 June 2018 relating to the processing of personal data (“personopplysningsloven”).

and follow the same routines as the bank's employees in Norway. DNB also stated that its main establishment is located in Norway, and that the decisions on the purposes and means of the relevant processing are taken in that establishment, which has the power to have such decisions implemented.

In light of the above, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case. Further, given that DNB's main establishment is located in Norway, Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. Therefore, a draft of the present decision was shared with the other supervisory authorities concerned, which did not raise any objections within a period of four weeks after having been consulted in accordance with Article 60(3) GDPR.

6. Datatilsynet's Assessment

At the outset, it must be pointed out that, in accordance with Article 29 GDPR, any person acting under the authority of the controller who has access to personal data may process those data only on instructions from that controller.

Moreover, it should be noted that information on the frequency and intensity of the consultation operations carried out by the employees of the controller may enable the data subject to ensure that the processing carried out is actually motivated by the purposes put forward by the controller.⁵

However, the CJEU has made clear that data subjects do not enjoy an absolute right to obtain from the controller information relating to the identity of the employees who carried out those operations.⁶ This is mainly because:

Even if the disclosure of the information relating to the identity of the controller's employees to the data subject may be necessary for that data subject in order to ensure the lawfulness of the processing of his or her personal data, it is nevertheless liable to infringe the rights and freedoms of those employees.⁷

Nonetheless, the CJEU stated that:

if the data subject were to consider the information provided by the controller to be insufficient to enable him or her to dispel his or her doubts as to the lawfulness of the processing of his or her personal data, he or she has the right to lodge a complaint with the supervisory authority on the basis of Article 77(1) of the GDPR, that authority having the power, under Article 58(1)(a) of that regulation, to request the controller to provide it with any information it needs in order to examine the data subject's complaint.⁸

⁵ CJEU, Case C- 579/21, *Pankki*, para. 70.

⁶ Ibid., para. 83.

⁷ Ibid., para. 79.

⁸ Ibid., para. 82.

It is in light of the above ruling, as well as the doubts expressed by the complainant, that Datatilsynet requested DNB to provide us with the information we needed to examine the complaint.

The information on the consultation operations carried out on the complainant's bank account since 17 May 2018 we obtained from DNB did not reveal any suspicious activity. Essentially all consultation operations were done in response to or in connection with a request from the complainant. No consultation operation had been carried out by someone employed at the "DnB Linderud" office. Moreover, most of the consultation operations had been carried out by male employees or a robot, and no single employee had carried out consultation operations with a very high frequency or intensity.

Therefore, the complainant's suspicions that a female employee of DNB's "DnB Linderud" office had carried out a large number of unauthorized accesses to her bank account appear to be unfounded.

Having considered the above, the complaint shall be rejected as unfounded in accordance with Article 60(8) GDPR.

7. Right of Appeal

As this decision has been adopted pursuant to Chapter VII GDPR, pursuant to Article 22(2) of the Norwegian Data Protection Act, the present decision may not be appealed before the Privacy Appeals Board (in Norwegian: *Personvernennemda*). However, the present decision may be challenged before Oslo District Court (in Norwegian: *Oslo tingrett*) in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act and Article 4-4(4) of the Norwegian Dispute Act (in Norwegian: *tvisteloven*).⁹

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

This letter has electronic approval and is therefore not signed

Copy to: DNB BANK ASA

⁹ See Section 22 of the Act of 15 June 2018 No. 38 relating to the processing of personal data (in Norwegian: *personopplysningsloven*).



Norwegian Data Protection Authority

[REDACTED]

*Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven
§ 24 første ledd 2. punktum .*

IMI reference
A60FD 632873

Our reference
21/04063

Date
24.04.2024

Rejection of complaint and closure of case – Zalando SE

The Norwegian supervisory authority (Datatilsynet) refers to your complaint dated 6 December 2021 regarding a credit check ordered by Zalando SE (Zalando). In a letter dated 10 May 2022, we informed you that this is a so-called cross-border case, which, according to data protection rules, is subject to different case handling procedures than ordinary cases.¹ The supervisory authority in Berlin, Germany has handled the case as lead supervisory authority because Zalando has its main establishment in Berlin. The supervisory authorities in Norway, Sweden, Denmark, Germany,² Finland, Poland, Spain, Austria, Luxembourg, France, Italy and Ireland have participated in the case as concerned supervisory authorities.

About the case handling

The Berlin supervisory authority has investigated the case by contacting Zalando. They have also asked for your feedback to the company's response. In cooperation with us and the other concerned supervisory authorities, they have assessed the case based on your complaint and other information you have provided, as well as the responses from the controller. In cooperation, we have made a decision. The case handling has followed the procedure in Article 60 GDPR, whereby the Berlin supervisory authority has presented a draft decision. We and the other concerned supervisory authorities agree with the Berlin supervisory authority's draft decision, and we are therefore adopting the final decision in line with their findings.

Our assessment

Datatilsynet closes the case with reference to the reasoning in the decision that follows below. The decision is written in English. We can assist with translation to Norwegian if needed. Please contact us if you need the decision translated.

¹ See the General Data Protection Regulation (GDPR) Art. 4(23) and Art. 56(1).

² The regional German supervisory authorities in the states North Rhine-Westphalia, Rhineland-Palatinate, Thuringia, Lower Saxony, Mecklenburg-Western Pomerania, Hesse, Saarland and Bavaria.

Decision

The investigation initiated in response to the above complaint has been completed. Based on the information provided, the Berlin DPA has not been able to establish an infringement of the General Data Protection Regulation (GDPR) in the processing of the complainant's personal data by the controller Zalando SE.

Reasoning:

I.

The Berlin DPA has established the following facts:

The complainant stated that they had created a customer account with the controller on 24 November 2021. The complainant did not place an order. However, they were informed by a letter from Experian AS dated 24 November 2021 that the controller had carried out a credit check of them. The complainant sent the Berlin DPA a copy of the notification. In addition, the complainant informed the Berlin DPA that their customer account shows that they are not offered the payment method 'purchase on invoice'.

On the occasion of the notification about the credit check, the complainant contacted customer service by email on 27 November 2021, expressly pointing out that they had not made a purchase. Customer service informed the complainant that the controller was carrying out credit checks to check whether the 'purchase on invoice' payment method could be offered. The customer service could inform them that if the complainant no longer wished to have credit checks carried out, the 'purchase on invoice' payment method would no longer be available (customer service emails dated 27 and 28 November 2021). Customer service also explained that the complainant had agreed to credit checks being carried out when the complainant had registered with the controller by accepting the terms and conditions and the privacy policy (customer service email dated 28 November 2022).

The Berlin DPA asked the controller for a statement on the matter. In a statement dated 7 July 2022, the controller informed the Berlin DPA that credit checks are not carried out independently of orders. Credit checks are only carried out in connection with a specific order if a risky payment method ('purchase on invoice') is selected.

Since June 2021, credit checks in Norway have only been carried out after a customer has placed goods in the shopping cart, entered their delivery and billing address, selected 'purchase on invoice' in the check-out process and confirmed this by clicking on the 'Continue' button. Clicking the 'Continue' button is the last step in the checkout process before the final page with the order summary appears. Then, the final completion of the order follows by clicking on the 'Confirm' button.

In the course of the order or checkout process, the customer is initially offered all possible payment methods. If the customer selects ‘purchase on invoice’, they are asked to enter their Social Security Number. The Social Security Number is then used to check the credit rating with Experian AS, based in Oslo. Customers are also informed of this. The controller provided the Berlin DPA with a screenshot of the Norwegian order page.

In the present case, the controller assumes that the complainant wanted to place an order after registering and selected the corresponding goods and the payment method ‘purchase on invoice’. Furthermore, the controller assumes that the order was not completed because the order process was cancelled. The legal basis for the credit check is Art. 6(1)(b) or (f) GDPR (not consent pursuant to Art. 6(1)(a) GDPR). With regard to the communication between the complainant and customer service, the controller stated that some of the responses from the relevant employees did not correspond to the internal templates and training. The case in question was taken as an opportunity to clarify how the misinformation could have occurred.

We have informed the Norwegian DPA of the state of affairs and asked them to inform the complainant accordingly. The Berlin DPA has also asked the complainant to inform the Berlin DPA if the facts presented by the controller are incorrect.

The Norwegian DPA forwarded to the Berlin DPA the complainant’s email dated 17 October 2022. In it, the complainant states that the information provided by the controller was incorrect. However, the complainant then describes that they placed an order with the controller immediately after creating the account on November 24, 2021 and wanted to pay for it ‘on invoice’. This was blocked by the controller and the complainant was only able to pay by credit card.

In the complaint, the complainant alleges that there was no legal basis for the credit check at Experian AS by the controller.

II.

Our legal assessment of the facts of the case is as follows:

With regard to the performance of the credit check, based on the information provided, the Berlin DPA was unable to establish an infringement by the controller in the processing of the complainant’s personal data.

The legal basis for carrying out a credit check is Art. 6(1)(f) GDPR. The avoidance of payment defaults constitutes a legitimate interest of the controller within the meaning of Art. 6(1)(f) GDPR. However, data processing for the purposes of the legitimate interest can only be considered necessary if there is a credit risk. However, a credit risk only exists if and when a customer selects a product, goes through the purchase process and actually selects a payment method that requires the controller to make advance payments, as is the case with the ‘purchase on invoice’ payment method.

When designing the order process, it must be ensured that credit checks are not carried out if a risky payment method is not clicked on at all or only inadvertently.

Against this background, the ordering process in Norway described by the controller at the time of the alleged infringement is not objectionable with regard to the performance of credit checks. The performance of a credit check can be based on Art. 6(1)(f) GDPR. The controller's legitimate interest was the avoidance of payment defaults. Carrying out a credit check was also necessary to safeguard this legitimate interest if the credit check was only carried out in connection with a specific order and only after selecting the payment method 'purchase on invoice', as the existence of a credit risk for controllers can then be assumed. In addition, the requirement to enter the Social Security Number and the requirement to click on the 'Continue' button ensures that a credit check is not carried out if a person inadvertently clicks on 'purchase on invoice'.

In the present case, the complainant confirmed that they initially wanted to order the goods 'on invoice' and only cancelled the order process when this was not possible. The Berlin DPA was therefore unable to establish that the actual ordering process did not correspond to the ordering process presented by the controller. On the contrary, this was confirmed.

Insofar as the complainant stated that they have not ordered anything, this does not per se remove the legal basis for carrying out a credit check. It should be noted that carrying out a credit check is not only necessary after the final placement of an order within the meaning of Art. 6(1)(f) GDPR, but under the above-mentioned conditions already during the ordering process in order to be able to check the existence of a risk of non-payment on the seller's side before the order is completed.

We therefore cannot establish an infringement of Art. 6(1) or Art. 5(1)(a) GDPR.

III.

Based on this assessment, the Berlin DPA assumes that no infringement of data protection regulation has actually occurred in the present case. The case is closed pursuant to Art. 60(8) GDPR.

As far as the complaint is concerned, the Berlin DPA considers the matter to be closed.

Ability to appeal

This decision has been adopted by us in accordance with Article 56 and Chapter VII GDPR, and can therefore not be appealed to the Norwegian Privacy Appeals Board pursuant to Section 22(2) of the Norwegian Personal Data Act (*personopplysningsloven*). This decision can nevertheless be challenged before Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Trine Smedbold
Senior Legal Adviser

This document is signed electronically and therefore includes no handwritten signatures.

[REDACTED]

*Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven
§ 24 første ledd 2. punktum .*

IMI reference
A60FD 632894

Our reference
22/03769

Date
24.04.2024

Rejection of complaint and closure of case – Zalando SE

The Norwegian supervisory authority (Datatilsynet) refers to your complaint dated 13 June 2022 regarding a credit check ordered by Zalando SE (Zalando). In a letter dated 18 August 2022, we informed you that this is a so-called cross-border case, which, according to data protection rules, is subject to different case handling procedures than ordinary cases.¹ The supervisory authority in Berlin, Germany has handled the case as lead supervisory authority because Zalando has its main establishment in Berlin. The supervisory authorities in Norway, Sweden, Denmark, Germany,² Finland, Poland, Spain, Austria, Luxembourg, France, Italy and Ireland have participated in the case as concerned supervisory authorities.

About the case handling

The Berlin supervisory authority has investigated the case by contacting Zalando. In cooperation with us and the other concerned supervisory authorities, they have assessed the case based on your complaint and other information you have provided, as well as the responses from the controller. In cooperation, we have made a decision. The case handling has followed the procedure in Article 60 GDPR, whereby the Berlin supervisory authority has presented a draft decision. We and the other concerned supervisory authorities agree with the Berlin supervisory authority's draft decision, and we are therefore adopting the final decision in line with their findings.

Our assessment

Datatilsynet closes the case with reference to the reasoning in the decision that follows below. The decision is written in English. We can assist with translation to Norwegian if needed. Please contact us if you need the decision translated.

¹ See the General Data Protection Regulation (GDPR) Art. 4(23) and Art. 56(1).

² The regional German supervisory authorities in the states North Rhine-Westphalia, Rhineland-Palatinate, Thuringia, Lower Saxony, Mecklenburg-Western Pomerania, Hesse, Saarland and Bavaria.

Decision

The Berlin DPA has concluded the investigation in the present case. A violation of the GDPR with regard to the processing of the complainant's personal data could not be identified.

Reasoning

I.

We have established the following facts:

The complainant, who is resident in Norway, has argued that on 13 May 2022, Zalando SE (the controller) carried out a credit check on him without his consent in connection with an order made via the controller's shop. The complainant had selected Vipps as a type of payment for the order. Vipps is a Norwegian payment app. Experian AS informed him about the conduct of the credit check. In a previous order in 2021, the complainant had used the payment type "purchase on invoice" and, upon request, the customer service informed the complainant that he had agreed to the credit assessment when selecting the payment type "purchase on invoice".

As evidence, the complainant provided a copy of the notification of Experian AS of 13 May 2022 and an order confirmation from the controller dated 17 May 2022. It follows from the latter that the complainant selected Vipps as the type of payment. The Berlin DPA also was provided with copied emails from the controller's customer service of 18 May 2022, 07:33, 18 May 2022, 10:49, 18 May 2022, 13:06, 18 May 2022, 13:48, 18 May 2022, 15:09 and 19 May 2022, 08:03.

The Berlin DPA heard the controller for their opinion. In their comments of 8 September 2023, the controller informed the Berlin DPA that the complainant had made an order in 2021 with the payment type "purchase on invoice". At the time of the order in May 2022, this type of payment had been pre-selected on the basis of the previous order from 2021. The complainant confirmed the choice of the payment type "purchase on invoice" in the new order by clicking on the 'further' button. By clicking on 'further', the choice of the type of payment was confirmed and the creditworthiness assessment was triggered. The complainant then dropped an order step within the ordering click and changed the payment type to 'Vipps' and finally completed the purchase with Vipps. The legal basis for the creditworthiness check is Article 6(1)(b) and (f) GDPR. The legitimate interest of controllers is the prevention of defaults, the detection of fraud and the investigation of criminal offences.

The controller also informed the Berlin DPA that the payment type 'purchase on invoice' could be permanently removed as a possible type of payment if a customer so wished. With regard to the communication between the complainant and the customer service, the controller stated that the information provided by the customer service did

not meet the current requirements of controllers, as the situation had been described to the complainant on the basis of the old process in force until June 2021.

Until June 2021, credit rating queries were based on consent. However, in June 2021, the process in Norway was changed in such a way that creditworthiness queries only happen after a customer placed goods in the basket, entered his delivery and invoice address, selected in the checkout process ‘Purchase on invoice’ and confirmed this input by clicking on the ‘further’ button.

The controller informed the Berlin DPA that the staff of the customer service would be provided with templates and FAQs to respond to customer requests. However, in the present case, the employees have answered the complainant’s questions in their own words. The controller took the opportunity of the present case to instruct employees once again to take account only of the templates when answering questions and dealing with customer concerns. In addition, the controller is planning to extend the drafting templates and FAQs to include further use cases.

II.

From a legal point of view, the Berlin DPA assesses the facts as follows:

The Berlin DPA was not able to establish an infringement by the controller in the processing of the complainant’s personal data on the basis of the information provided.

The legal basis for carrying out a credit assessment is Article 6(1)(f) GDPR. The prevention of defaults constitutes a legitimate interest for the controller within the meaning of Article 6(1)(f) GDPR. In the present case, however, data processing based on the legitimate interest is to be regarded as necessary only if there is a credit risk. However, a credit risk exists only when a customer selects a good, goes through the purchase process and actually selects a type of payment for which the controller has to make an advance payment, as is the case for the payment type ‘purchase on invoice’. In the design of the ordering process, it is therefore necessary to ensure that credit checks are not carried out simply if a risk-related payment type is not selected at all or is only accidentally selected.

The ordering process in Norway described by the controller at the time of the alleged infringement is not to be contested in this respect with regard to the conduct of creditworthiness queries. The performance of a credit assessment can be based on Article 6(1)(f) of the GDPR. The legitimate interest of the controller was, *inter alia*, to avoid defaults. It was also necessary to carry out a credit test in order to safeguard that legitimate interest, provided that, as argued by the controller, the creditworthiness check was carried out only in connection with a specific order and only after the payment type ‘purchase on invoice’ has been selected, since it can then be assumed that there is a credit risk for the controller.

In so far as the complainant claimed that they had completed the purchase with Vipps, the controller confirmed this. However, the controller added that the complainant first selected the payment type ‘purchase on invoice’ by clicking on the ‘further’ button. The creditworthiness check should therefore be based on Article 6(1)(f) of the GDPR on the basis of the information available to the Berlin DPA. The fact that the type of payment ‘purchase on invoice’ had been pre-received on the basis of the complainant’s previous order cannot be criticised – provided that the selection was actually made by the respective customer – which is to be assumed in the present case, as the complainant also stated that he made the order from 2021 with the payment type ‘purchase on invoice’.

In that regard, it should be noted that the carrying out of a credit assessment is not to be regarded as necessary only after the final placing of an order within the meaning of Article 6(1)(f) of the GDPR, but, under the above conditions, even during the ordering process, in order to be able to verify the existence of a risk of non-payment on the seller’s side.

The Berlin DPA therefore cannot identify an infringement of Article 6(1) and Article 5(1)(a) of the GDPR.

III.

On the basis of this assessment, the Berlin DPA finds that there has indeed been no violation of data protection rules in the present case. The proceedings are concluded in accordance with Article 60(8) of the GDPR.

As far as the complaint is concerned, the Berlin DPA considers the matter to be closed.

Ability to appeal

This decision has been adopted by us in accordance with Article 56 and Chapter VII GDPR, and can therefore not be appealed to the Norwegian Privacy Appeals Board pursuant to Section 22(2) of the Norwegian Personal Data Act (*personopplysningsloven*). This decision can nevertheless be challenged before Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Trine Smedbold
Senior Legal Adviser

This document is signed electronically and therefore includes no handwritten signatures.



Norwegian Data Protection Authority

[REDACTED]

*Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven
§ 24 første ledd 2. punktum .*

IMI reference
A60FD 632908

Our reference
20/01756

Date
24.04.2024

Rejection of complaint and closure of case – Zalando SE

The Norwegian supervisory authority (Datatilsynet) refers to your complaint dated 13 August 2018 regarding a credit check ordered by Zalando SE (Zalando). In emails dated 8 January 2019 and 16 May 2019, we informed you that this is a so-called cross-border case, which, according to data protection rules, is subject to different case handling procedures than ordinary cases.¹ The supervisory authority in Berlin, Germany has handled the case as lead supervisory authority because Zalando has its main establishment in Berlin. The supervisory authorities in Norway, Sweden, Denmark, Germany,² Finland, Poland, Spain, Austria, Luxembourg, France, Italy and Ireland have participated in the case as concerned supervisory authorities.

About the case handling

The Berlin supervisory authority has investigated the case by contacting Zalando. In cooperation with us and the other concerned supervisory authorities, they have assessed the case based on your complaint and other information you have provided, as well as the responses from the controller. In cooperation, we have made a decision. The case handling has followed the procedure in Article 60 GDPR, whereby the Berlin supervisory authority has presented a draft decision. We and the other concerned supervisory authorities agree with the Berlin supervisory authority's draft decision, and we are therefore adopting the final decision in line with their findings.

Our assessment

Datatilsynet closes the case with reference to the reasoning in the decision that follows below. The decision is written in English. We can assist with translation to Norwegian if needed. Please contact us if you need the decision translated.

¹ See the General Data Protection Regulation (GDPR) Art. 4(23) and Art. 56(1).

² The regional German supervisory authorities in the states North Rhine-Westphalia, Rhineland-Palatinate, Thuringia, Lower Saxony, Mecklenburg-Western Pomerania, Hesse, Saarland and Bavaria.

Decision

We hereby inform you that the investigation initiated in response to the above-mentioned complaint has been concluded. Based on the information provided to us, we have not been able to establish an infringement of the General Data Protection Regulation (GDPR) in the processing of the complainant's personal data by the controller Zalando SE.

Justification:

I.

We have established the following facts:

The above-mentioned complainant, represented by her mother, submitted a complaint about Zalando SE (Controller) to the Data Protection Authority in Norway on 13 August 2018. The complainant alleged that the controller had carried out a credit check in August 2018 without cause. Upon request, customer service informed the complainant that the controller checks the creditworthiness of customers once or twice a year, regardless of purchase.

In a statement dated 10 May 2019, the controller informed us that credit checks are not carried out independently of orders. Credit checks are only carried out in connection with a specific order if the payment method 'purchase on account' is selected.

In Norway, the process would be as follows: If a new customer has placed goods in the shopping basket, the customer would be offered possible payment methods in the order process (checkout). If the customer selects 'purchase on account', they are asked to enter their Social Security Number. The Social Security Number is then used to check the credit rating with Experian AS, based in Oslo.

For existing customers, a credit check is only carried out if more than 180 days have passed since the last order process and the customer initiates an order process again and selects 'purchase on account'. If the last order process has taken place within the last 180 days, the controller uses the existing creditworthiness values to decide whether the 'purchase on account' payment method is possible.

With regard to the complainant, the controller stated in a statement dated 14 October 2021 that a credit check had been carried out for the complainant's customer account on 4 August 2018 at 11:22 PM. The controller assumes that an order process was initiated with the complainant's customer account, but was not completed. In this respect, the controller submitted an excerpt from the event logs. The event logs submitted show that a login to the complainant's customer account took place on 4 August 2018 at 21:21:42. The legal basis for the credit check is Art. 6 para. 1 lit. b or f GDPR.

In a statement dated 12 January 2022, the controller added that since June 2021, credit checks in Norway have only been carried out after a customer has placed goods in the shopping cart, entered their delivery and billing address, selected ‘purchase on account’ in the checkout process and confirmed this by clicking on the ‘Continue’ button. Clicking the ‘Continue’ button is the last step in the checkout process before the final page with the order summary appears. Then, the final completion of the order follows by clicking on the ‘Confirm’ button.

II.

Our legal assessment of the facts of the case is as follows:

We were unable to establish an infringement by the controller Zalando SE in the processing of the complainant’s personal data on the basis of the information provided to us.

Art. 6(1)(f) GDPR can be considered as the legal basis for carrying out a credit check. The avoidance of payment defaults constitutes a legitimate interest of the controller within the meaning of Art. 6(1)(f) GDPR. However, data processing for the purposes of the legitimate interest is only considered necessary in the present case if there is a credit risk. Yet, a credit risk only exists if and when a customer selects a product, goes through the purchase process and actually selects a payment method that requires the controller to make advance payments, as is the case with the ‘purchase on account’ payment method. When designing the ordering process, it must be ensured that credit checks are not carried out in cases where a risky payment method is not clicked on at all or only inadvertently.

The ordering process in Norway described by the controller at the time of the alleged infringement is not objectionable in this respect with regard to the performance of credit checks. The performance of a credit check can be based on Art. 6(1)(f) GDPR. The controller’s legitimate interest was the avoidance of payment defaults. Carrying out a credit check was also necessary to safeguard this legitimate interest if the credit check, as submitted by the controller, was only carried out in connection with a specific order and only after selecting the payment method ‘purchase on account’, as the existence of a credit risk for the controller can then be assumed. In addition, the requirement to enter the Social Security Number ensures that a credit check is not carried out if a person inadvertently clicks on ‘purchase on account’.

We were unable to establish that the actual ordering process did not correspond to the ordering process presented by the controller. The complainant claimed that the controller had carried out a credit check in August 2018, although she had not ordered anything. Although the controller confirmed that the credit check was carried out on 4 August 2018 at 11:22 PM, it denied that the credit check was carried out without cause. Instead, the controller argued that it was assumed that an order process had

been started but ultimately not completed. By submitting the event logs, the controller has comprehensibly demonstrated that the complainant's customer account was active, i.e. logged in, at the time of the credit check. It therefore appears at least possible that a purchase process was initiated that legitimately led to the credit check of the complainant. In particular, the complainant has not argued that she was not active on the controller's website on the evening of 4 August 2018.

Insofar as the complainant has argued that she did not order anything, it should be noted that a credit check is not only necessary within the meaning of Art. 6(1)(f) GDPR after the final placement of an order, but under the above-mentioned conditions already during the ordering process in order to be able to check the existence of a risk of non-payment on the seller's side.

We therefore cannot establish an infringement of Art. 6(1) or Art. 5(1)(a) GDPR.

III.

Based on this assessment, we assume that no infringement of data protection regulations has actually occurred in the case available for review. The proceedings are terminated pursuant to Art. 60(8) GDPR.

As far as the complaint is concerned, we consider the matter to be closed.

Ability to appeal

This decision has been adopted by us in accordance with Article 56 and Chapter VII GDPR, and can therefore not be appealed to the Norwegian Privacy Appeals Board pursuant to Section 22(2) of the Norwegian Personal Data Act (*personopplysningsloven*). This decision can nevertheless be challenged before Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Trine Smedbold
Senior Legal Adviser

This document is signed electronically and therefore includes no handwritten signatures.

[REDACTED]

*Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven
§ 24 første ledd 2. punktum .*

IMI reference
A60FD 632324

Our reference
21/01484

Date
24.04.2024

Rejection of complaint and closure of case – Zalando SE

The Norwegian supervisory authority (Datatilsynet) refers to your complaint dated 12 April 2021 regarding credit checks ordered by Zalando SE (Zalando). In an email dated 1 October 2021, we informed you that this is a so-called cross-border case, which, according to data protection rules, is subject to different case handling procedures than ordinary cases.¹ The supervisory authority in Berlin, Germany has handled the case as lead supervisory authority because Zalando has its main establishment in Berlin. The supervisory authorities in Norway, Sweden, Denmark, Germany,² Finland, Poland, Spain, Austria, Luxembourg, France, Italy and Ireland have participated in the case as concerned supervisory authorities.

About the case handling

The Berlin supervisory authority has investigated the case by contacting Zalando. They have also asked for your feedback to the company's responses. In cooperation with us and the other concerned supervisory authorities, they have assessed the case based on your complaint and other information you have provided, as well as the responses from the controller. In cooperation, we have made a decision. The case handling has followed the procedure in Article 60 GDPR, whereby the Berlin supervisory authority has presented a draft decision. We and the other concerned supervisory authorities agree with the Berlin supervisory authority's draft decision, and we are therefore adopting the final decision in line with their findings.

Our assessment

Datatilsynet closes the case with reference to the reasoning in the decision that follows below. The decision is written in English. We can assist with translation to Norwegian if needed. Please contact us if you need the decision translated.

¹ See the General Data Protection Regulation (GDPR) Art. 4(23) and Art. 56(1).

² The regional German supervisory authorities in the states North Rhine-Westphalia, Rhineland-Palatinate, Thuringia, Lower Saxony, Mecklenburg-Western Pomerania, Hesse, Saarland and Bavaria.

Decision

I.

The above-mentioned complainant, based in Norway, submitted that the controller Zalando SE (controller) had checked its creditworthiness with Experian AS at regular intervals without cause, in particular not in connection with an order. The complainant was informed by Experian AS about the credit checks by the controller and in this respect submitted copies of notifications from Experian AS dated 9 April 2018, 23 October 2018, 23 June 2018, 25 September 2019, 20 March 2020, 30 September 2020, 30 March 2021 and 26 April 2022.

Although the complainant was a customer of the controller, she had only placed orders with the controller on 30 December 2014 and 25 September 2019. On 2 October 2020, the complainant called customer service to request the erasure of her customer account. On the same day, customer service asked the complainant by e-mail to provide three out of six details for comparison or to send an e-mail from the e-mail address stored in the customer account in order to be able to carry out the erasure. The complainant did the latter on 5 October 2020. Customer service then informed the complainant by email that her customer account had been deactivated and would be deleted in five days. Nevertheless, the complainant received a notification of a credit check by the controller from Experian AS on 30 March 2021 and most recently on 26 April 2022. The complainant was also able to continue logging into her customer account.

In a statement dated 9 August 2022, the controller informed the Berlin DPA that an internal investigation had revealed that two customer accounts with the controller had been created with the complainant's social security number. In addition, there were further matches in the two customer accounts, including name, date of birth, gender, and in some cases also the delivery and billing address.

The controller has stated that no routine credit checks are carried out, but only in connection with a specific order when selecting the risky payment method "purchase on account". The legal basis for the credit check is Art. 6 (1) (b) or (f) GDPR.

An order was placed on 25 September 2019 via the customer account with the number A [redacted], in which the above-mentioned e-mail address of the complainant (A [redacted]@gmail.com) was stored. The payment method "purchase on account" was selected.

Orders were placed on 20 March 2020, 30 September 2020, 30 March 2021 and 26 April 2022 via the second customer account with the number B [redacted], in which the e-mail address B [redacted]@gmail.com was stored, for which the payment method "purchase on account" was also selected.

On a further three days (9 April 2018, 23 June 23 2018 and 23 October 2018), a login to the customer account with the number B [redacted] took place, but no order was placed. The controller assumes that the order process was cancelled in the last step of the check-out process. A total of 33 orders were placed from this customer account between 2017 and 2022, thirty of which were placed using the "purchase on account" payment method.

With regard to the request for erasure, the controller stated that the customer account with the number A [redacted] had not been erased. The controller was no longer able to fully clarify why the account had not been erased. In this respect, the controller submitted that the screenshots provided by the complainant did not reveal the sender and recipient of the emails. The communication with the complainant was no longer available for the controller. The facts of the case could therefore no longer be fully clarified. It is possible that the erasure was not carried out due to the duplicate account management. The customer account with the number A [redacted] was finally deactivated on 2 August 2022.

The Berlin DPA informed the DPA in Norway of the content of the statement on 14 September 2022 and asked them to inform the complainant of the current status. In particular, the Berlin DPA asked the DPA in Norway to ask the complainant whether the controller's statements are correct and whether the complainant is the holder of both customer accounts. The Berlin DPA also asked for the complete email communication between the complainant and the controller.

In a letter dated 2 January 2023, the DPA in Norway informed the Berlin DPA that the complainant had replied that the customer account with the number A [redacted] belonged to her daughter [redacted]. The complainant had created the account for her daughter when she was still a minor. The daughter is now 22 years old. The complainant had confirmed that the above-mentioned orders had been placed by her daughter. She suspected that some of her personal data was still linked to the customer account.

The Norwegian DPA stated that it was assumed that the complaint regarding the performance of the credit checks had now been resolved for the complainant.

Finally, the complainant stated that the customer account with the number B [redacted], which her daughter uses, should be reactivated. With regard to the customer account with the number A [redacted] used by her, she continued to request erasure.

II.

The Berlin DPA's legal assessment of the facts of the case is as follows:

With regard to the performance of the credit checks, the Berlin DPA assumes that the facts of the case have been clarified to the satisfaction of the complainant and that the subject matter of the complaint has been resolved.

Irrespective of this, the Berlin DPA was unable to establish an infringement by the controller in the processing of the complainant's personal data on the basis of the information provided to the Berlin DPA, as the credit checks mentioned above were probably carried out lawfully on the basis of Art. 6 (1) (f) GDPR. At least insofar as the credit check, as submitted by the controller, was only carried out in connection with a specific order and only after selecting the payment method "purchase on account", as in this case it can be assumed that the controller has an overriding legitimate interest.

The complainant confirmed the above-mentioned orders by herself or her daughter and admitted that she had created both customer accounts herself. In this respect, the Berlin DPA assumes that the complainant has also deposited her Social Security Number in both customer accounts. Therefore, there is no reason to doubt the controller's statements available in this case. The Berlin DPA is therefore unable to establish an infringement of Art. 6 (1), Art. 5 (1) (a) GDPR.

With regard to the request for erasure, the Berlin DPA cannot prove an infringement of Art. 17 (1) GDPR by the controller, as the corresponding communication between the complainant and the controller was not submitted to the Berlin DPA in full or could no longer be submitted to the Berlin DPA. In addition, due to the duplication of customer accounts using the same Social Security Number, it seems at least possible that the controller could invoke an exemption from the erasure obligation pursuant to Art. 17 (3) (b) or (e) GDPR. In any case, after submitting the complaint to the DPA in Norway, the controller should be able to invoke the exception pursuant to Art. 17 (3) (e) GDPR.

Insofar as the controller has informed the Berlin DPA that the complainant has informed them that the customer account used by her daughter with the number B [redacted] is to be reactivated, while the customer account used by the complainant with the number A [redacted] is to be deleted, the Berlin DPA requests the complainant to contact the controller again with reference to the conclusion of the present investigation.

With regard to the granting of access to the customer account, the Berlin DPA would like to point out that the reactivation of the customer account or a possible claim to access to the account is regulated in the terms of use, which are regularly agreed to when the customer account is set up. This is an agreement under civil law between the respective customer and the controller. The enforcement of rights and claims arising from this must be asserted by civil law if necessary.

III.

Based on this assessment, the Berlin DPA assumes that no infringement of data protection regulations has actually occurred in the present case. The case is closed pursuant to Art. 60 (8) GDPR.

As far as the complaint is concerned, the Berlin DPA consider the matter to be closed.

Ability to appeal

This decision has been adopted by us in accordance with Article 56 and Chapter VII GDPR, and can therefore not be appealed to the Norwegian Privacy Appeals Board pursuant to Section 22(2) of the Norwegian Personal Data Act (*personopplysningsloven*). This decision can nevertheless be challenged before Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Trine Smedbold
Senior Legal Adviser

This document is signed electronically and therefore includes no handwritten signatures.

HURTIGRUTEN GROUP AS
Langkaia 1
0150 OSLO

Exempt from public disclosure:
Offl. § 20 første ledd B

Your reference

Our reference
21/02687-7

Date
16.05.2024

'Sui Generis' Decision - Hurtigruten

On 27 July 2021, the Hamburg Commissioner for Data Protection and Freedom of Information (“Hamburg SA”) shared with the Norwegian Data Protection Authority (“Datatilsynet”, “us”, “our”) a complaint that [REDACTED] (the “complainant”) lodged against Hurtigruten Group AS (“controller”) with the Hamburg SA.

In March 2021, the controller wrote to the complainant to inform her about a data security incident that affected the complainant’s passport information that the controller collected in 2018.

Following this communication, on 15 March 2021, the complainant wrote to the Hamburg SA to complain about the excessive retention of her personal data from the part of the controller. The complaint was shared through the Internal Market Information System (IMI) on 27 July 2021, and Datatilsynet was identified as the lead supervisory authority within the meaning of Article 56(1) GDPR.

Further to our inquiry, it appears that some of the personal data of the complainant had indeed been retained longer than was actually necessary for the purposes for which the personal data had been processed. However, the controller informed us that this excessive retention of personal data was due to an occasional oversight from their part, which the controller has acknowledged and remedied since the complaint was lodged in 2021.

We have therefore sought to facilitate an amicable settlement with the controller in accordance with Recital 131 GDPR, and encouraged the controller to reach out to the complainant for this purpose.

On 29 February 2024, the controller wrote to the complainant to explain that the excessive retention of her passport data was due to an occasional breach of the controller’s internal routines, and to apologize for any inconvenience caused. The controller also offered the complainant to cover any expenses related to the change of passport, and to provide further assistance in relation to the incident.

In light of the above, and given that the complainant has not responded to the above-mentioned letter, we consider that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR, and that the matter may be deemed to be resolved to the complainant's satisfaction. We have therefore decided to close the present case in accordance with Article 60(7) GDPR and the requirements of Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021).

A draft of the present decision was shared with the complainant and with the other supervisory authorities concerned in accordance with Article 60(3) GDPR. None of them has raised any objections.

Kind regards,

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

This letter has electronic approval and is therefore not signed

Copy to: Complainant
 HmbBfDI

SATS ASA
Postboks 4949 NYDALEN
0423 OSLO

*Exempt from public disclosure:
Offl. § 13, jf. personopplysningsloven § 24 første ledd 2.
punktum*

Your reference

Our reference
24/00844-10

Date
20.08.2024

Final Decision - SATS ASA

1. Introduction and Factual Background

On 15 December 2023, the Norwegian Data Protection Authority (hereinafter “Datatilsynet”, “we”, “our”, “us”) received a complaint against SATS ASA (hereinafter “SATS”) from the Swedish Authority for Privacy Protection (hereinafter “IMY”) (Case 24/00844). The complaint was submitted by [REDACTED], a member of the fitness centers run by SATS in Sweden (hereinafter “complainant”), who essentially claimed that SATS violated Regulation (EU) 2016/679 (hereinafter “GDPR”) as:

- SATS has unlawfully transferred personal data to a debt collection agency (Lowell Sverige AB, hereinafter “Lowell”), and has not informed the competent data protection authority about this.
- SATS has not responded to a request for erasure of his personal data transferred to Lowell that the complainant sent to SATS on 12 January 2023.
- SATS’ privacy policy does not provide sufficient information, as it does not spell out exactly what personal data SATS processes and to which specific third countries such personal data may be transferred.
- With respect to the processing of personal data of SATS members in Sweden, the controller mentioned in the privacy policy is not the Swedish entity with whom the Swedish members have a contractual relationship.

Further to our inquiry, SATS informed us that, in January 2023, the complainant contacted SATS to inform them about an invoice that he incorrectly received from SATS’ debt collection supplier (i.e., Lowell) and to request that all of his personal data processed in connection with the issuing of the invoice at hand be deleted.

The evidence produced by SATS shows that, in January 2023, SATS contacted Lowell to request them to annul the invoice at issue and to delete all personal data of the complainant. Furthermore, the evidence produced by SATS shows that, on 12 January 2023, SATS informed the complainant that the invoice had been annulled and that no payment was due, and offered him two months of free membership as a compensation for any inconvenience caused.

However, SATS acknowledged that it failed to properly inform the data subject about the deletion of his personal data. It noted that this was due to an occasional breach of its internal routines, which will be taken into account to improve SATS' routines in the future. SATS confirmed though that all personal data of the complainant have been deleted by Lowell, and that only a copy of the incorrectly issued invoice has been kept by SATS for mere bookkeeping purposes. On 27 February 2024, after we opened our inquiry, SATS informed the complainant about this.

SATS also informed us that it updated its privacy policy on 23 May 2023 (and again on 29 February 2024), after receiving on 6 February 2023 a fining decision that sanctioned SATS for several violations of the GDPR, including for violations of data subject rights and transparency requirements partially analogous to those mentioned in the complaint.¹

Furthermore, SATS told us that it did not consider the transfer of personal data to Lowell as a reportable personal data breach under Articles 33 or 34 GDPR.

On 4 March 2023, the complainant wrote to IMY to inform them that, in his view, the action taken by SATS had not fully resolved the compliance issues identified in his complaint. The complainant also raised a few additional issues (e.g., an alleged lack of reply to an access request he submitted on 11 January 2023), which have not been dealt with as part of the present case, as they were not part of the original complaint. However, we trust that SATS will review all previous correspondence with the complainant to make sure that there are no responses that are still due to him.

2. Datatilsynet's Competence

Based on information provided by SATS in previous cases,² SATS runs a chain of fitness centers. It has its headquarter in Norway, but has also operations and offices in Denmark, Finland and Sweden.

Thus, SATS has several establishments in the EU/EEA, including in Norway, and in the context of the activities of these establishments it processes personal data, including the personal data of its customers, such as the complainant. Therefore, the GDPR applies to such data processing activities in accordance with Article 3(1) GDPR.

The SATS group has its main establishment (within the meaning of Article 4(16) GDPR) in Norway. Moreover, the processing of the personal data of SATS members, including the

¹ See Datatilsynet's decision No 20/02422-9 of 6 February 2023.

² Ibid.

complainant, qualifies as cross-border processing under Article 4(23) GDPR. This is because, SATS members' personal data may be accessed by SATS' staff in all of the European countries in which SATS operates, and SATS' internal routines and policies are the same in all of the European countries in which SATS operates.

Therefore, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to the present case, and Datatilsynet is competent to act as lead supervisory authority in the case at hand pursuant to Article 56(1) GDPR. This was not disputed by SATS in the course of our inquiry.

As a result, pursuant to Article 60(3) GDPR, a draft of the present decision was shared with the other supervisory authorities concerned, which did not raise any objections.

3. Datatilsynet's Assessment and Decision

With respect to the complainant's arguments on the lack of sufficient information in SATS' privacy policy regarding the kinds of personal data processed by SATS, it should be noted that listing all categories of personal data concerned is not required *per se* under Article 13 GDPR, whereas it is expressly required under Article 14 GDPR.³ This is because the provision of information on the categories of personal data concerned is especially relevant when "the personal data has not been obtained from the data subject, who therefore lacks an awareness of which categories of their personal data the data controller has obtained".⁴ However, providing information on the specific categories of personal data processed may be necessary also when the personal data have been collected from the data subject to comply with the transparency principle in Article 5(1)(a) GDPR.

While it is true that, as argued by the complainant, SATS' privacy policy does not – and did not – spell out all kinds of personal data that SATS processes, it provides – and provided – several examples of personal data and categories of personal data concerned (e.g., name, gender, age, exercise history, health data, etc.). This may "avoid information fatigue".⁵ Moreover, it should be noted that the personal data to be processed for issuing invoices (e.g., name, address, bank account details) do not include special categories of personal data and are typically obtained from the data subjects who are thus generally aware of them.

Therefore, the information provided in SATS' privacy policy about the kind of personal data processed by SATS does not appear to be insufficient to meet the GDPR's transparency requirements, at least with respect to the information to be provided to the complainant under Article 13 GDPR regarding invoicing and debt collection activities. To the extent that Article 14 GDPR is applicable, the fact that SATS did not spell out all the categories of personal data to be processed is a rather minor violation that we trust SATS will remedy by further updating its privacy policy. In this context, it should also be noted that the current version of SATS' privacy policy expressly states that personal data may be shared with Lowell:

³ See Article 14(1)(d) GDPR.

⁴ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, p. 36.

⁵ *Ibid.*, p. 7.

In English: “We may also share information with other suppliers who act as data controllers, such as Lowell our debt collection partner.”

In Swedish: “Vi kan också dela information med andra leverantörer som agerar som behandlingsansvariga, såsom Lowell, vår partner för inkassotjänster”.

As for the information on transfers of personal data to third countries, it is true that, as argued by the complainant, SATS’ privacy policy (or at least the version in Swedish) in effect before the latest update in February 2024 did not provide any information on international data transfers.

This would be a clear violation of Article 13(1)(f) GDPR, if at that time SATS transferred personal data to third countries. However, this has not been investigated in the present case, given that the complainant’s personal data have been transferred to an entity in Sweden (i.e., Lowell).

The current version of SATS’ privacy policy states:

In English: “We may transfer your personal data outside the EEA in certain situations, as some of our suppliers (or sub-suppliers) and business partners may be located in such countries. We will ensure that your data is secured by adopting appropriate safeguards to protect the privacy (such as EU’s Standard Contractual Clauses). We will provide you with further details about such international data transfers upon request. If you want to obtain a copy of the safeguards, please use the contact details below.”

In Swedish: “Vi kan överföra dina personuppgifter utanför EES i vissa situationer, eftersom några av våra leverantörer (eller underleverantörer) och affärspartners kan vara belägna i sådana länder. Vi kommer att säkerställa att dina data är säkrade genom att anta lämpliga skyddsåtgärder för att skydda integriteten (såsom EU:s Standardavtalsklausuler). Vi kommer att tillhandahålla dig ytterligare detaljer om sådana internationella datatransferer vid begäran. Om du vill erhålla en kopia av skyddsåtgärderna, vänligen använd kontaktuppgifterna nedan.”

This wording is insufficient to ensure full compliance with the transparency requirements set out in the GDPR. This is because “[i]n accordance with the principle of fairness, the information provided on transfers to third countries should be as meaningful as possible to data subjects; this will generally mean that the third countries be named.”⁶ However, the fact that the relevant third countries are not named in SATS’ privacy policy is a rather minor violation that we trust SATS will remedy by further updating its privacy policy.

As for the transfer of the complainant’s personal data to Lowell, we take note of SATS’ argument that this was due to an occasional mistake affecting a single data subject, which – in

⁶ Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, Adopted on 29 November 2017, As last Revised and Adopted on 11 April 2018, p. 38.

their view – was unlikely to result in a risk to the rights and freedoms of natural persons, and was thus not a reportable personal data breach under Articles 33 or 34 GDPR. During the investigation, we found no evidence to dispute this conclusion. SATS was made aware of the mistake by the affected data subject himself – who was thus aware of it – and immediately took action to correct it and avoid any negative consequences for the data subject (e.g., undue payments). Moreover, the personal data at issue were transferred to one of SATS’ regular suppliers – and not to an unknown third party – who promptly deleted the personal data concerned after having been notified of the mistake by SATS. Due to these facts this data breach was unlikely to result in a risk to the rights and freedoms of the data subjects, hence no notification to the competent supervisory authority or the concerned data subject was necessary. However, this data breach must be documented in accordance with Article 33(5) GDPR.⁷

In this regard, it should be noted that the transfer of personal data to a debt collection agency to pursue a debt on behalf of a controller does not generally give rise to specific data protection concerns, as the transfer may normally take place on the basis of Article 6(1)(b) or (f) GDPR.⁸

As to the complainant’s argument that the controller mentioned in SATS’ Swedish privacy policy was not the Swedish entity with whom Swedish members have a contractual relationship, we note that this fact is not in itself strange or problematic, as the controller does not necessarily need to be the local contractual counterparty, in particular where the local entity is part of a larger multinational group where decisions about personal data processing are taken centrally. In any event, after the latest update in February 2024, SATS privacy policy in Swedish now states that “SATS Sports Club Sweden AB” is the controller with respect to the processing of personal data of Swedish members:

In Swedish: “SATS Sports Club Sweden AB (‘SATS’, ‘vi’, ‘vår’, ‘oss’) driver en kedja av gym och relaterade tjänster (såsom SATS Online, SATS-appen och SATS-webbplatsen). Denna integritetsnotis ger dig information om vår behandling av personuppgifter som ansvarig för personuppgifter.”

We have not investigated as part of the present case whether this update reflects today’s factual reality regarding decision-making on means and purposes of personal data processing. However, we understand that, at least in the past, decisions on means and purposes of the processing of personal data in all of the countries where SATS operates were entirely or at least partially made in Norway. We would thus encourage SATS to review this to make sure that what is indicated in the Swedish privacy policy reflects the actual allocation responsibilities and decision-making within the SATS group.

With respect to the complainant’s erasure request, SATS itself has acknowledged that it did not appropriately respond to such a request. Indeed, SATS failed to provide information on the action taken on the request without undue delay and in any event within one month of receipt of the request, in violation of Article 12(3) GDPR. However, this may be considered a relatively minor violation, as SATS did take action on the request; it only failed to properly inform the

⁷ See by analogy EDPB, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Adopted on 14 December 2021, Version 2.0, paras. 114-118.

⁸ See, e.g., the judgment of Administrative Court of Mainz of 20 February 2020 (VG Mainz - 1 K 467/19.MZ).

data subject about it. Moreover, SATS has eventually provided information on the action taken to the data subject on 27 February 2024, although it did so in Norwegian. Even though Scandinavian languages are generally mutually intelligible, communications with data subjects should normally occur in their language to ensure that the communication is provided in “clear and plain language” as required by Article 12(1) GDPR. We trust that SATS will take note of this for any future communication with data subjects.

Finally, it should be noted that the violations identified in the present case have taken place before SATS was fined for partially similar violations on 6 February 2023.⁹ Therefore, they were presumably linked to the systemic compliance issues for which SATS has already been fined in our decision of 6 February 2023, which has led SATS to upgrade its data protection policies and routines.

In light of the above, Datatilsynet is of the view that, despite the rather minor violations identified, it is not necessary to adopt any corrective measures against SATS in the present case. In this respect, it should be noted that there is no obligation on supervisory authorities to impose corrective measures in all cases or when the complainant so requests.¹⁰ Nonetheless, we trust that SATS will take note of and remedy all violations identified by updating its data protection policies and routines.

However, this decision is without prejudice to the possibility of opening future inquiries into SATS’ compliance with data subject rights, and the lawfulness and transparency requirements set out in the GDPR, including with respect to the updates to its privacy policy that SATS is expected to undertake in light of the present decision.

4. Right of Appeal

As this decision has been adopted pursuant to Article 56 and Chapter VII GDPR, pursuant to Article 22(2) of the Norwegian Data Protection Act, the present decision may not be appealed before Personvernemda. However, the present decision may be challenged before Oslo District Court (“Oslo tingrett”) in accordance with Article 78(1) GDPR, Article 25 of the Norwegian Data Protection Act and Article 4-4(4) of the Norwegian Dispute Act.¹¹

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

⁹ See Datatilsynet’s decision No 20/02422-9 of 6 February 2023.

¹⁰ See Opinion of Advocate General Pikamäe in Case C-768/21, TR v Land Hessen.

¹¹ Act of 17 June 2005 no. 90 relating to mediation and procedure in civil disputes (Lov om mekling og rettergang i sivile tvister (tvisteloven)).

This letter has electronic approval and is therefore not signed

LEA BANK ASA
Holbergs gate 21
0166 OSLO

Deres referanse

Vår referanse

24/01427-11

Dato

19.08.2024

Sui Generis Decision - LEA Bank ASA

On 1 April 2024, the Spanish Agency for Data Protection (“Agencia Española de Protección de Datos”, “ES SA”) shared with the Norwegian Data Protection Authority (“Datatilsynet”, “us”, “our”) a complaint lodged by [REDACTED] (“complainant”) against LEA Bank ASA (“LEA Bank”, “bank”, “controller”).

The complainant argued that on 21 November 2023 he contacted LEA Bank to essentially obtain the deletion of the personal data he submitted to the bank in connection with a request for a loan that LEA Bank rejected. However, according to the complainant, he received no response from LEA Bank.

Further to our inquiry, LEA Bank acknowledged that they have received a request for a loan from the complainant on 21 November 2023, but they do not seem to have received the request concerning the complainant’s personal data.

In any event, LEA Bank informed us that their internal routines and policies provide for the automatic deletion of the personal data submitted in connection with requests for a loan that LEA Bank has rejected. LEA Bank has confirmed that the complainant’s personal data have been deleted as part of this standard process.

Taking into account that the automatic erasure of the complainant’s personal data has essentially mooted the issues raised in the complaint, that supervisory authorities «should seek an amicable settlement with the controller» (Rec. 131 GDPR), and that on 11 July 2024 the ES SA has informed the complainant of the above without receiving any objections regarding the closure of the case, we consider that the subject matter of the complaint has been investigated to the extent appropriate in accordance with Article 57(1)(f) GDPR, and that the matter may be deemed to be resolved to the complainant’s satisfaction. We have therefore decided to close the present case in accordance with Article 60(7) GDPR and the requirements of Internal EDPB Document 06/2021 on the practical implementation of amicable settlements (adopted on 18 November 2021).

Pursuant to Article 60(3) GDPR, a draft of the present decision was shared with the supervisory authorities concerned, which did not raise any objections.

Kind regards

Tobias Judin
Head of International

Luca Tosoni
Specialist Director

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturen

Kopi til: Supervisory Authorities Concerned

NORWEGIAN AIR SHUTTLE ASA
Postboks 115
1330 FORNEBU

Your reference

Our reference
20/02288-43

Date
16.09.2024

Decision to issue a reprimand – Norwegian Air Shuttle ASA

1. Introduction and Summary

The Norwegian Data Protection Authority (hereinafter “**Datatilsynet**”, “we”, “us”, “our”) is the independent supervisory authority responsible for monitoring the application of the General Data Protection Regulation (“**GDPR**”)¹ with respect to Norway.

We received a complaint against Norwegian Air Shuttle ASA (hereinafter “**NAS**”, “you”, “your”). The complaint concerned alleged infringements of facilitating data subject rights committed by NAS, in particular in connection with the verification of data subjects pursuant to Article 12.

After having investigated the complaint, we are of the view that NAS infringed Articles 12(2), 12(6) and 5(1)(c) GDPR.

2. Datatilsynet’s Decision

Pursuant to Article 58(2)(b) GDPR, we hereby adopt the following decision:

Datatilsynet issues Norwegian Air Shuttle ASA with a reprimand for:

- *Infringing Article 12(6) GDPR by requesting the provision of the complainant’s photo ID without demonstrating that it had reasonable doubts as to the identity of the complainant*
- *Infringing Article 5(1)(c) GDPR by requesting more information than was necessary in order to confirm the identity of the data subject*

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ [2016] L 119/1.

- *Infringing Article 12(2) GDPR by effectively imposing unnecessarily burdensome measures on the complainant by requiring provision of photo ID in order to carry out the complainant's request*

We are competent to issue corrective measures pursuant to Article 58(2) GDPR.

3. Factual Background

On 26 September 2018, we received (via the Finnish Data Protection Authority) a complaint from a data subject in Finland (the “**complainant**”) against NAS in relation to NAS’ processing of the complainant’s personal data.

The complainant was a customer of NAS who had received a marketing e-mail from NAS on 22 May 2018. On 25 May 2018, the complainant contacted NAS through an online channel and asked NAS for a full statement of all the records it has of the complainant and why, and for clarification as to how the complainant can remove this information from NAS’ records.

NAS responded on 11 June 2018 from the e-mail address "data.protection@norwegian.com" stating that in order for NAS to reply to the complainant’s request it must obtain additional information from the complainant in order to verify the complainant’s identity, and requested the complainant to upload a copy of their valid identification document containing their photo (“**Photo ID**”) by using a link to NAS’ online form.

On 18 June 2018, the complainant sent a complaint to the Finnish Data Protection Authority questioning whether NAS had the right to request a copy of their passport before fulfilling their access request (the “**Complaint**”).

On 11 October 2018, we sent an order to provide information to NAS based on the Complaint, specifically aimed at the appropriateness and necessity of NAS requesting data subjects for a copy of their Photo ID in order to verify the identity of the data subject making a request.

On 7 November 2018, NAS responded to our order to provide information dated 11 October 2018 and stated, amongst other things, that it:

- processes a number of different categories of personal information and for varying lengths of time, referring to its privacy policy then applicable.
- does not require that a data subject identifies themselves in order to manage a data subject's consents.
- carried out a risk assessment in order to secure compliance with applicable data protection laws, taking into account amongst other things:
 - it processes the personal data of approximately 45 million customers,
 - many e-mail addresses do not contain a specific name,
 - the owner of e-mail addresses may change over time, and
 - many trips are ordered by persons other than those who will travel.

- therefore considers e-mail addresses themselves as not sufficient to confirm the identity of a data subject.
- considers that a copy of accepted identification documents as the best possible verification of a data subject, and if NAS are still unable to identify the data subject or there are duplicate findings, it requests further information such as last trip travelled etc.
- considers that the consequences of disclosing a data subject's personal data to an incorrect person is more severe than the burden of requesting additional information.

On 11 April 2019, NAS had a physical meeting with us to discuss the contents of NAS' response to our order to provide information and potential solutions. Further to such meeting, NAS sent an e-mail to us on 21 May 2019 stating that NAS had assessed the issue and sees that it is unfortunate that additional information is collected to allow individuals to exercise their rights under the GDPR, even though NAS considers it is important to ensure personal data is not sent to the wrong person. NAS further stated that they consider it is important that approved identification documents showing the data subject's name is shown, and proposed a potential solution where individuals could redact all superfluous information (such as the picture and social security number) from the copy of their identification document before submitting it to NAS.

On 20 June 2019, we circulated a draft decision to the other supervisory authorities concerned pursuant to Article 60(3) GDPR and proposed to close the matter without further action being taken on the condition that NAS carry out their proposed solution as outlined above and explain or give examples to data subjects as to how they may redact their approved identification document. A number of supervisory authorities concerned disagreed with such draft decision by raising objections or comments. The objections and comments of supervisory authorities concerned were summarised in a letter to NAS dated 30 April 2021 as follows:

- Controllers may not impose unnecessary or excessive procedural burdens on data subjects that wish to exercise their rights under the GDPR, and shall instead make it as easy as possible for data subjects to exercise their rights under the GDPR.

The reasoning for such disagreement was summarised in a letter to NAS dated 30 April 2021, and we ordered NAS to provide further information by answering the following questions (translated from the original Norwegian text):

1. *Do you carry out an individual assessment regarding whether there exists reasonable doubt as to the identity of the data subject that wishes to exercise their rights pursuant to Article 15-21 [GDPR]? If so, we request that you attach your routines for this assessment.*
2. *Do you carry out an individual assessment regarding what additional information which is required to confirm the identity of the data subject? If so, we request that you attach your routines for this assessment and how this occurs in practice.*
3. *Regarding the requirement to provide a copy of a passport:*

- a. *Do you still require a copy of an identification document to confirm the identity of those that wish to exercise their rights, including those that wish to be removed from a newsletter?*
 - b. *If so, have you implemented the change you proposed in the meeting of 11 April 2019, including the solution where individuals redact all superfluous information in the approved identification document*
 - c. *If the provision of a copy of a passport is necessary for all data subjects that wish to exercise their rights, how do you assess this as against Article 5(1)(c) [GDPR]?*
4. *Facilitation of the exercise of data subject rights:*
- a. *We request that you explain in more detail how you facilitate data subjects' ability to exercise their rights pursuant to Articles 15-21 [GDPR], pursuant to Article 12(2) [GDPR].*
 - b. *We request that you explain and attach screenshots of the "flow" on your website so that we see how the system looks from the data subject's perspective. We request that you also explain if the "flow" is the same for the exercise of all rights or if it is differentiated.*

On 11 June 2021, NAS responded to our order to provide information dated 30 April 2021 stating that it:

- updated its routines after meeting with us on 11 April 2019 to inform data subjects that they may redact all information except their name and the issuer from a copy of their valid identification document. NAS also acknowledged the need to differentiate between different types of data subject requests as, for example, wrongfully sharing personal data to those other than the data subject is not applicable to erasure requests.
- now has different routines for different types of data subject requests, namely:
 - In relation to access requests, NAS requests data subjects to provide a copy of their valid identification document but informs data subjects that they may redact all information save for their name and the name of the issuer of the valid identification document. Furthermore, if the data subject is not comfortable providing NAS with a copy of their valid identification document, NAS uses e-mail address to verify data subjects and limits the access provided to only personal data connected to the applicable e-mail address. NAS may also provide information based solely on a data subject's travel reference information.
 - In relation to erasure requests, NAS requests the data subject's e-mail address and conducts the erasure based on this. If in doubt, NAS' customer care may request additional information from the data subject such as travel reference information.
 - In relation to correction requests, NAS requests the data subject's e-mail address or travel reference information.
 - In relation to objection requests, NAS' data protection officer handles these and the verification of the data subject is based on an individual assessment.
 - In relation to newsletter requests, this is handled without verification.

- does not carry out an individual assessment as to whether a name or e-mail enables identification due to the number of requests received and the numerous possibilities related to both names and e-mails, particularly as there may be several people with the same name and many e-mails do not contain any names but often abbreviations. NAS does however carry out an individual assessment based on what the customer is comfortable sharing.
- shared copies of screenshots showing the "flow" as referenced in our order to provide information. For access requests, the screenshot shows that NAS requires the data subject to upload a copy of a valid identification document in order to identify the data subject, and states all information except the name and issuer may be redacted.

On 22 June 2021, NAS provided us with further information stating it:

- only requests a copy of a redacted valid identification document for data subject access requests.
- has initiated several GDPR projects:
 - The right to be forgotten project to ensure compliance with the requirements of Article 17 GDPR. This involves allowing the data subject to order erasure of their own data online without the involvement of NAS' customer care centre. The data subject is identified either through them logging on to their online account or through e-mail verification, potentially also with further verification e.g. by text message.
 - Consent management (marketing activities and newsletter) is handled through an online based e-mail form or the data subject's online account.
 - The access project, which will implement a new solution enabling data subjects to automatically order and receive a copy of their personal data – although noting that the verification method to be used is not yet finalised although verification could take place e.g. through text message.

On 20 August 2021, we ordered NAS to provide further information by answering the following questions (translated from the original Norwegian text):

1. *We request that you explain in more detail the ongoing GDPR activities relating to the identification of data subjects, including which changes are proposed in the on-going "GDPR projects" (in addition to that which is contained in your letter of 21 June 2021).*
2. *In an e-mail dated 21 June 2021, Linda Methlie writes:*
 - A data subject can delete all information on their ID except issuer and name. This solution acv id [sic] will be replaced by a new solution which will use another method to verify the data subject (e.g. sms). Other data subject rights pursuant to the GDPR are handled without requiring ID. Does this mean that the solution requiring providing ID will be discontinued and replaced by a new solution? If so, we request you explain in more detail this solution. If the new solution involves changes to how you assess whether "reasonable doubt" as to the identity of a data subject exists, we request you to also explain this.*

3. *We request that you explain in more detail how a data subject can say that they do not wish to provide their ID (even with redactions). On your website it does not look like the data subject has any choice.*
4. *What has happened with the Finnish complainant in this case? Was he removed from the newsletter? Did he receive access to his personal data/have his personal data deleted? If so, how long did it take from when he sent in such requests to when they were resolved?*

On 7 September 2021, NAS responded to our order to provide information dated 20 August 2021 stating that:

- The new solutions relating to the right to be forgotten and the right to access own data will involve including a button on customer accounts to "forget me" and to "access my data". The verification method will be logging on to the customer account. This requires new IT solutions and will involve adjustment in all of NAS' systems that process personal data and external third parties processing personal data on behalf of NAS.
 - For customers without an online account, the identification requirements have not yet been decided upon, but an automated process is the targeted end result meaning that there will not be a requirement to provide ID. The identification of correct data subjects is part of an ongoing DPIA and will be concluded based on the risks identified in the DPIA.
- In relation to the current system of receiving access requests, NAS added that there is a text field where the data subject may object to NAS' requirement to upload a copy of (potentially redacted) ID, and that the request process does not stop if no ID is uploaded.
- In relation to the Finnish complainant, NAS stated that it cannot find any case relating to them in the customer care system which means that they have not submitted a request through NAS' portal. However, the complainant does not receive a newsletter from NAS.

On 27 September 2022, NAS sent us a letter stating that in light of this matter, NAS undertook a further review and assessment of the practice of requiring ID from data subjects in relation to the exercise of data subject rights. Based on such assessment, NAS concluded that they no longer require ID to verify the identity of a data subject in relation to the exercise of data subject rights.

On 14 July 2023, we sent NAS with an advance notice of our intention to adopt a decision to issue a reprimand and invited their comments. NAS responded on 9 August 2023 that they did not have any comments further to their letter of September 2022.

On 11 August 2023, we submitted a draft decision to the other supervisory authorities concerned. The supervisory authority that had originally received the complaint had certain comments to such draft decision, in particular regarding how the issue had been resolved regarding the complainant.

On 30 August 2023, we withdrew the draft decision from IMI due to comments from one supervisory authority. Shortly afterwards, we sent NAS an order to provide information as to how the complainant's original access request had been handled, and whether NAS still processed the complainant's data. If NAS had not handled the complainant's original request, we requested NAS to make contact with the complainant to confirm their details and arrange for a copy of their personal data to be sent to the complainant. In addition, we also asked NAS to confirm with the complainant whether or not they wished to exercise their right to erasure.

On 8 September 2023, NAS responded and stated they could not confirm whether the original request had been complied with and that they could confirm that the complainant still had an active profile with them. NAS further stated that they would contact the complainant again to ensure that complainant's requests are complied with.

The complainant responded to NAS on 4 February 2024 confirming that they wished to exercise their right to access under Article 15 GDPR and then deletion under Article 17 GDPR.

On 12 February 2024, NAS confirmed that the complainant's access and erasure request were complied with on 9 February 2024. At our request, the supervisory authority that received the original complaint contacted the complainant to ask whether they were satisfied with the measures taken by the controller to respect their rights. The complainant did not respond to the complaint receiving supervisory authority within the deadline set.

4. Legal Background

The GDPR has been incorporated into Annex XI to the European Economic Area ("EEA") Agreement by means of Decision of the EEA Joint Committee No 154/2018 ("EEA Joint Committee Decision").²

Article 1(b) of the EEA Joint Committee Decision provides that:

"[...] the terms "Member State(s)" and "supervisory authorities" shall be understood to include, in addition to their meaning in the Regulation, the EFTA States and their supervisory authorities, respectively."

Further, Article 1(c) of the EEA Joint Committee Decision reads as follows:

"References to Union law or Union data protection provisions shall be understood as referring to the EEA Agreement or data protection provisions contained therein, respectively."

² Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement OJ [2018] L 183/23.

The Norwegian Personal Data Act (*Nw. personopplysningsloven*) incorporated the GDPR into Norwegian law.³ The Norwegian Personal Data Act and the GDPR entered into force in Norway on 20 July 2018.⁴

Article 5(1)(c) and (2) GDPR reads as follows:

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');*
...
2. *The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').*

Article 12(2) and (6) GDPR reads as follows:

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.*
...
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.*

5. Datatilsynet's Competence

NAS is established in Norway and in the context of its activities it processes personal data. Therefore, the GDPR applies to NAS' data processing activities in accordance with Article 3(1) GDPR.

With respect to the processing of the personal data of the complainant, NAS qualifies as a controller within the meaning of Article 4(7) GDPR, as NAS decided on the means and purposes of the relevant processing of personal data, as acknowledged in NAS' privacy policy at the time of the complaint.⁵

³ Act No 38 of 15 June 2018 relating to the processing of personal data ("personopplysningsloven").

⁴ Ibid., § 32.

⁵

<https://web.archive.org/web/20180425231647/https://www.norwegian.no/booking/bestillingsinformasjon/regler-og-vilkar/personvern/>

As a controller, NAS has its main establishment within the meaning of Article 4(16) GDPR in Norway. Moreover, the processing of the personal data of NAS customers, including the complainant, qualifies as cross-border processing under Article 4(23) GDPR. This is because the policies and routines of NAS in relation to the exercise of data subject rights, and more particularly the verification of data subjects, substantially affect or are likely to substantially affect data subjects in more than one EEA state.

Therefore, the cooperation mechanism and procedure set out in Articles 56(1) and 60 GDPR apply to this case and we are competent to act as lead supervisory authority pursuant to Article 56(1) GDPR.

6. The Norwegian Data Protection Authority's assessment

Chapter 3 of the GDPR lays down the rights of data subjects. These rights allow data subjects to retain control over their personal data that is processed by controllers. The right of access under Article 15 GDPR is one of the rights that a data subject can exercise against a controller.

We consider that the complainant's e-mail to NAS dated 25 May 2018 was an access request pursuant to Article 15 GDPR, and that NAS itself interpreted such e-mail as a data subject right request as it responded to the complainant on 11 June 2018 from the e-mail address "data.protection@norwegian.com" requesting additional information from the complainant for the purposes of verifying the identity of the data subject in order for NAS to comply with the request.

Pursuant to Article 12(2) GDPR a controller must facilitate the exercise of the rights of data subjects and shall not refuse to act on the request of a data subject to exercise his or her rights, unless the controller demonstrates that it is not in a position to identify the data subject. In other words, it must be demonstrably impossible for the controller to be able to identify the data subject based on the information already in its possession at the time it receives the data subject request in order to be able to validly refuse to act.

Any verification method must be proportionate to the objective to be achieved, in this case to provide the data subject with access to their personal data pursuant to Article 15 GDPR, and limited to what is necessary in relation to such purpose, i.e. that the purpose cannot reasonably be fulfilled by less harmful or less intrusive means in accordance with Article 5(1)(c) GDPR. Controllers should implement or re-use an authentication procedure in order to ascertain the identity of the data subjects requesting their personal data or exercising the rights granted by the GDPR insofar as a digital communication channel already exists between the data subject and the controller. In this case, a digital communication channel already existed between the complainant and NAS, in that the complainant's e-mail address was stored in NAS' systems and NAS used the complainant's e-mail address to communicate with the complainant when responding to the complainant's data subject request. Therefore NAS possessed the information it needed to be able to identify the data subject at the time of the Complaint.

If a controller is able to identify the data subject based on the information it already has in its possession, but nevertheless has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject pursuant to Article 12(6) GDPR. It follows that a controller that wishes to rely on Article 12(6) GDPR must therefore conduct a two-stage assessment. Firstly, a controller must determine whether it has reasonable doubts concerning the identity of the natural person making a data subject request. Secondly, if reasonable doubts as to the identity of the person making a data subject request exist, a controller must determine what additional information is *necessary* to be able to confirm the identity of the data subject in accordance with the principle of data minimisation.

NAS did not at the time of the Complaint carry out any individual assessment as to whether it had reasonable doubts regarding the identity of the complainant making a request under Article 15 GDPR. NAS required the complainant to upload an un-redacted copy of their Photo ID before NAS would proceed with responding to the complainant's request. Further, NAS did not inform the complainant that there was any other way of identifying themselves.

We therefore consider that NAS has not demonstrated that it had reasonable doubts as to the complainant's identity in accordance with Article 12(6) GDPR that would have justified it requesting the complainant to provide additional information in order to confirm their identity. Neither do we consider that NAS requesting a copy of the complainant's Photo ID was necessary or proportionate in accordance with Article 5(1)(c) GDPR under the circumstances where there were less intrusive ways of confirming the complainant's identity. NAS could have used other authentication methods to confirm the identity of the data subject without having to resort to requiring the data subject to upload an unredacted copy of their valid Photo ID, such as asking the complainant security questions based on travel history.

In light of the above, we therefore find that NAS:

- Infringed Article 12(6) GDPR by requesting the provision of the complainant's Photo ID without demonstrating that it had reasonable doubts as to the identity of the complainant
- Infringed Article 5(1)(c) GDPR by requesting more information than was necessary in order to confirm the identity of the data subject
- Infringed Article 12(2) GDPR by effectively imposing unnecessarily burdensome measures on the complainant by requiring provision of Photo ID in order to carry out the complainant's request

7. Mitigating factors

NAS has throughout our investigation of the Complaint been cooperative and shown willingness to adjust its routines and policies where necessary.

NAS changed their routines shortly after meeting with us in 2019 to discuss the problems raised by the Complaint, and further changed their routines in 2021 following the comments

of the Danish and Finnish data protection authorities to NAS' practice. In September 2022, NAS informed us that after having undertaken a further review and assessment of the verification of data subjects, NAS no longer requires data subjects to submit a copy of an identification document in relation to the exercise of data subject rights.

8. Corrective Measures

In light of the extent of the infringements identified and taking into account the mitigating factors above, we consider it is appropriate to issue NAS with a reprimand pursuant to Article 58(2)(b) GDPR.

9. Access to Case Documents and Public Access

As a party to the present case, you have the right to access the documents in this case pursuant to Section 18 of the Norwegian Public Administration Act⁶.

All documents we possess are subject to freedom of information requests pursuant to Article 3 of the Norwegian Freedom of Information Act.⁷ If you believe that this letter or your written representations should be partly or fully exempt from public access, please let us know and explain why you believe such an exemption should be applied.

10. Right of Appeal

As this decision has been adopted by Datatilsynet pursuant to Article 56 and Chapter VII GDPR, it is not possible to appeal it before the Norwegian Privacy Appeals Board pursuant to Section 22 of the Norwegian Personal Data Act (*Nw. personopplysningsloven*). This decision may nevertheless be appealed before the Norwegian courts in accordance with Article 78(1) GDPR.

Kind regards

Tobias Judin
Head of Section

Sebastian Forbes
Senior Legal Adviser

This letter has electronic approval and is therefore not signed

Copy to: the complainant

⁶ Lov 10. februar 1967 om behandlingsmåten i forvaltingssaker (forvaltningsloven).

⁷ Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemde (offentleglova) § 3.

[REDACTED]

Exempt from public disclosure:

*Offl. § 13, jf. personopplysningsloven § 24 første ledd 2.
punktum*

Your reference

Our reference

Date

20/02270-12

22.10.2024

Closure of case

Datatilsynet refers to your complaint dated 19 November 2019 regarding lack of erasure of personal data, and Datatilsynet's letter to you dated 5 July 2024 where we requested your feedback in the case.

Decision

Datatilsynet rejects your complaint.

Background

We informed you on 21 January 2020 that this is a so-called cross-border case. The case is cross-border because & Other Stories is established in more than one EEA country and the processing in question takes place in the context of the activities of such establishments. To ensure uniform application of the GDPR in the EEA, data protection authorities across the EEA must cooperate in the handling of cross-border cases.

The Swedish Data Protection Authority has acted as lead supervisory authority in the handling of your complaint. We, and 12 other supervisory authorities, have been involved as concerned supervisory authorities.

Reasoning for our decision

The Swedish supervisory authority has investigated the subject matter of your complaint to the extent appropriate in accordance with Article 57(1)(f) GDPR and, based on such

Postal address:

Office address:

Phone:

Ent.reg:

Home page:

P.O. Box 458 Sentrum
N-0105 OSLO

Trelastgata 3
N-0191 OSLO

+47 22 39 69 00

974 761 467

www.datatilsynet.no/en/

investigation, they have not found any infringement of the GDPR. The Swedish supervisory authority has therefore concluded that your complaint should be rejected and that the case should be closed. All concerned supervisory authorities, including us, agree with such conclusion.

Please find below information from the Swedish supervisory authority. This information explains how your complaint has been handled and the reasons as to why your complaint should be rejected. As your complaint is to be rejected, the supervisory authority that received your complaint – in this case us – is the one which will adopt the final decision pursuant to Article 60(8) GDPR.

As this is a cross-border case, the information is written in English. We can provide a translation. If you wish to receive a translation, please contact us.

The Swedish Authority for data protection (IMY) has received a complaint from you against & Other stories/H&M Hennes & Mauritz AB. The complaint was transferred from the supervisory authority of the Member State where you lodged your complaint (Norway) in accordance with the provisions of the GDPR on cooperation in crossborder processing. IMY has handled the case as responsible supervisory authority for the company's operations pursuant to Article 56 of the GDPR.

IMY shall process complaints about incorrect processing of personal data and, where appropriate, investigate the subject matter of the complaint (Article 57(1)(f) GDPR). The CJEU has ruled that the supervisory authority must investigate such complaints with due care. According to 23 § of the Swedish Administrative Procedure Act (2017:900), an authority must ensure that a case is investigated to the extent required by its nature.

On 28th of June 2024 IMY asked the Norwegian supervisory authority to forward a letter asking you whether your complaint was still relevant. You were informed that if we do not receive an answer from you within the set timeframe we will presume that you no longer wish to pursue this concern and we will proceed to close our file in this matter.

IMY has not received any response from you. IMY therefore assumes that the complaint is no longer relevant. Against this background, IMY finds no reason to continue the investigation.

IMY closes the case.

For information purposes, IMY would like to inform you that you always have the opportunity to submit a new complaint to us.



Ability to appeal

This decision has been adopted by us in accordance with Article 56 and Chapter VII of the GDPR, and can therefore not be appealed to the Norwegian Privacy Appeals Board pursuant to Section 22(2) of the Norwegian Personal Data Act (*in Norwegian: personopplysningsloven*). This decision can nevertheless be challenged before Norwegian courts in accordance with Article 78(1) GDPR.

Duty of Confidentiality

Parties to this matter have a duty of confidentiality under Section 13(b) of the Norwegian Public Administration Act regarding the information they receive about the complainant's identity, personal matters and other identifying information, and such information can only be used to the extent necessary to safeguard their interests in this case. Any breach of this duty of confidentiality can be punished pursuant to Section 209 of the Norwegian Penal Code.

In light of the above, we have now closed our case on this matter.

Kind regards

Tobias Judin
Head of Section

Anne Eidsaa Hamre
Senior legal adviser

This document is electronically approved and therefore does not require a handwritten signature.

Postal address: Office address: Phone: Ent.reg: Home page:

P.O. Box 458 Sentrum Trelastgata 3 +47 22 39 69 00 974 761 467 www.datatilsynet.no/en/
N-0105 OSLO N-0191 OSLO



Case number: NAIH/2020/4044/6
Antecedent case No.: NAIH/2019/5418.
In charge: [REDACTED]

Attention [REDACTED]
[REDACTED]

Dear Sir,

On 29 May 2018, you lodged the complaint with the Romanian data protection authority, in which you presented that you received marketing messages from [REDACTED] (hereinafter: Controller) by e-mail. You attempted to unsubscribe the newsletter on several occasions and according to your complaint, in addition to unsubscribing, you requested the erasure of your e-mail address from the Controller also by e-mail without success as you continued to receive marketing messages. According to your complaint lodged with the Romanian data protection authority, you attempted to unsubscribe the newsletter on 24 May 2018 for the last time, yet you received the Controller's newsletter of 28 May 2018.

It was established under the procedure initiated by the Romanian data protection authority according to Article 56 of the General Data Protection Regulation that the Hungarian National Authority for Data Protection and Freedom of Information (hereinafter: Authority) is the lead supervisory authority in this case as the decisions concerning the purposes and instruments of the processing of personal data are made in Hungary within the Controller's organisation.

In its e-mail of 20 December 2018 sent to [REDACTED], the Authority requested you to make a statement within eight days whether the Authority may disclose your identity to the Controller in the course of the procedure and warned you that without disclosing your identity the investigation cannot be conducted. The Authority also requested you to send a copy of the erasure request addressed to the Controller and referred to in your complaint lodged with the Romanian supervisory authority and sent by e-mail, as well as copies of any other communications and correspondence with the Controller and the Controller's response to the erasure request, if any. With a view to your identification, the Authority called upon you to state your full name, your mother's name and place and date of birth to the Authority.

The Authority did not receive any answer from you to this inquiry. The Authority repeated its inquiry of 20 December 2018 with identical content on 28 July 2019 in an e-mail sent to [REDACTED] however, you did not respond to this inquiry either.

In the absence of a response from you, the Authority examined the documents and information made available to it by the Romanian data protection authority. It was not possible to establish from the screenshots enclosed when you unsubscribed the Controller's newsletter or on how many occasions as they are not dated and no other data are shown, from which the date of unsubscribing could be established, furthermore the e-mail messages, in which you requested the erasure of your e-mail address from the Controller according to your statement, were not available to the Authority either. Consequently, your statement according to which you unsubscribed the Controller's newsletter also on 24 May 2018 and that you requested the erasure of your e-mail address by e-mail were not in any way substantiated or verified.

The screenshots of the electronic newsletters of the Controller do not reveal who the addressee of these newsletters was and what e-mail address they were sent to by the Controller. Despite a newsletter sent after 24 May 2018 being included in the list, the above points remain unverified, and therefore no decision establishing an infringement can be based on it. Owing to the deficiencies of the facts of the case, the Authority took up contact with you by e-mail on two occasions, but you disregarded these inquiries.

Based on the above, the Authority rejects your complaint without an investigation of merit in accordance with Section 53(3)(c) of Act CXII of 2011 on the Right to Informational Self-Determination and the Freedom of Information as in the absence of evidence the complaint should be regarded as ungrounded.

Budapest, 25 June 2020.

Yours sincerely,

On behalf



Dr. Attila Péterfalvi
President

Honorary university professor

PRESIDENT
OF THE PERSONAL DATA PROTECTION
OFFICE
Jan Nowak

Warsaw, 9 March 2023

DS.523.467.2022.ZS.JKO.

DECISION

Pursuant to Article 104 §1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws 2022, item 2000 as amended), Art. 7(1) and (2) of the Act on Personal Data Protection of 10 May 2018 (Journal of Laws 2019, item 1781), in conjunction with Art. 58 (2)(b) and Article 12(3) and (4) in conjunction with Art. 17(1) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Journal of Laws EU L 119 of 04.05.2016, p. 1 and Journal of Laws of the EU L 127 of 23.05.2018, p. 2 and Journal of Laws UE L 74 of 4.03.2021, p. 35) (hereinafter: GDPR), having conducted an administrative proceedings concerning the complaint lodged by [REDACTED] (address: [REDACTED]) on irregularities in the processing of her personal data by company [REDACTED] with its registered office in Warsaw at [REDACTED], consisting in the failure to comply with the request to erase her personal data, President of the Personal Data Protection Office

provides a reprimand to company [REDACTED] with its registered office in Warsaw at [REDACTED] for violation of Article 12(3) and Article 17(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Official Journal of the EU L 119 of 4.05.2016, p. 1, Official Journal of the EU L 127 of 23.05.2018, p. 2, and Official Journal of the EU L 74 of 4.03.2021, p. 35), consisting in the failure to act promptly, and at the latest within one month, on the request to erase the personal data of [REDACTED] (address: [REDACTED]) from the website with URL address [REDACTED]

Justification

Personal Data Protection Office has received a complaint from the Spanish Supervisory Authority (hereinafter: Spain SA), through the Internal Market Information

System

(IMI)¹

via

an Article 56 notification under the number A56ID 356000.1 from [REDACTED]

[REDACTED] (address: [REDACTED])

[REDACTED], hereinafter the Complainant, regarding irregularities in the processing of her personal data by company [REDACTED] with its registered office in Warsaw at [REDACTED], hereinafter: the Company, consisting of failure to comply with the request to delete the Complainant's personal data processed on the website [REDACTED]

[REDACTED] regarding the e-mail address, password to the user's account (hidden using stars), name and surname, date of birth, address, telephone number and payment method. The Polish Supervisory Authority (hereinafter: Polish SA), which is the President of the Personal Data Protection Office (hereinafter PDPO), having analyzed the facts of the case, considered itself as the leading supervisory authority to conduct the present complaint case pursuant to Article 56(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation (Official Journal of the EU L 119 of 4.05.2016, p. 1, Official Journal of the EU L 127 of 23.05.2018, p. 2, and Official Journal of the EU L 74 of 4.03.2021, p. 35) hereinafter: GDPR, due to the registered office of the Company, which is located on the territory of Poland, as informed by the Spanish SA on 19 January 2022.

In the complaint, the Complainant indicated that she was a user of the service through which the Company operates, i.e. the website [REDACTED]. The Complainant also indicated that she wants to delete her account, but does not find a special button to perform this action, as mentioned in the "FAQs" section. The complainant stated that she sent two deletion requests to the mailbox that appears as the controller's contact information on the website, but received no response. The complainant also pointed out that she continues to receive emails with new surveys to fill out and can still log into her user account.

In the course of the investigation in the present case, the President of the PDPO, as the lead supervisory authority, obtained clarifications on the circumstances of the case and established the following facts.

1. The President of the PDPO on 9 May 2022, through the Spanish SA notified the Complainant that the present complaint case had been identified as having a cross-border nature in accordance with Article 4(23) of the GDPR and the President of the PDPO initiated an administrative investigation procedure and asked the Company to submit an explanation on the matter;
2. The President of the PDPO on 9 May 2022, requested the Company to respond to the content of the complaint and provide an explanation of the case;
3. In explanations submitted to the President of the PDPO on 19 May 2022, the Company indicated the following:
 - a. The Company currently does not process the Complainant's personal data on the website [REDACTED] as this data has been deleted by the Company. Before deletion, the Company processed the Complainant's personal data provided by the

¹ European Commission Internal Market Information System.

Complainant in the course of creating an account on the [REDACTED] website on the basis of:

- Article 6(1)(b) of the GDPR - the necessary for the performance of the agreement for the provision of account services, in order to create an individual account, manage this account and provide access to surveys and conduct billing of services provided under the concluded agreement, in terms of: e-mail address, address data (postal code), date of birth, gender;
 - Article 6(1)(a) of the GDPR - consent of the data subject for the performance of an agreement for the provision of a Newsletter service for the purpose of performing an agreement the subject of which is a service provided electronically, in the following scope: e-mail address;
 - Article 6(1)(f) of the GDPR - legitimate interest, for the purpose of establishing, investigating and enforcing claims and defending against claims in proceedings before courts and other state authorities, in terms of: name and surname, home address, telephone number, data on the use of services if the claims arise from the way the user uses the services, other data necessary to prove the existence of the claim, including the extent of the damage suffered;
- a. The Company pointed out that the Complainant had never been employed by the Company;
 - b. The Complainant sent an early email to the Company on 7 September 2021 requesting that her account be closed. Then on 14 September 2021 the Complainant sent a second email from the same email address to the Company regarding the processing of her personal data, indicating in the content an email address that did not appear in the Company's database;
 - c. The Company deleted all of the Complainant's personal data processed on the website [REDACTED] and on 19 May 2022 responded to both of the Complainant's messages confirming the full implementation of the request made by the Complainant, as proof of which it attached 2 screenshots showing the full content of the Company's correspondence with the Complainant;
 - d. The Company explained that the delay in processing the Complainant's request was caused by a technical error consisting in the incorrect classification of messages from the Complainant by the e-mail server, as a result of which the Complainant's messages were moved to the SPAM folder. Immediately upon receiving information about the incident in question, the Company performed an investigation of the circumstances of the case and took all available measures to ensure the highest possible level of personal data protection, compliance with data protection regulations and to prevent similar situations in the future. The Company stressed that the technical error that caused the incident had been analyzed, the Complainant's personal data had been deleted, and a response had been given to the correspondence sent by the Complainant. As a result of the deletion of the Complainant's account, the Company also stopped sending emails to the Complainant containing invitations to complete the survey;
 - e. The Company indicated that it conducted a detailed review of the correctness of the processing of personal data in terms of the legal basis, purposes and scopes, and the updating of such data. The Company stressed that in order for the scope of

- personal data in particular to comply with the principle of data minimization indicated in Article 5(1)(c) of the GDPR, as a result of this analysis it decided to collect less personal data and to make a comprehensive update of personal data stored in the Company's database. The update consisted of deleting currently stored redundant personal data (as redundant data, personal data about which there could be any doubt in demonstrating the correct legal basis was classified) in the form of: telephone number and address data in terms of street name and house/apartment number;
- g. The Company stated that corrective procedures have been put in place involving the use of new technical solutions to improve communication with the customer and speed up the processing of the data subject's request for deletion of personal data. On the website: [REDACTED] in the customer panel, a new solution was added and tested in the form of an account deletion button that allows direct and independent account deletion;
 - h. The Company stated that the Complainant's personal data was also processed on the basis of consents given by the Complainant via the website when setting up an account on the website: [REDACTED]. With regard to the Complainant's consent to receive a newsletter, the Company pointed out that it had discontinued the newsletter service and the Complainant had never received commercial information within the meaning of the Act of 18 July 2002 on electronic services;
 - i. The Company stated that when processing personal data in the course of its business, it makes every reasonable effort to ensure the safety of personal data processing, compliance with the provisions of the GDPR and other data protection laws, and the realization of the rights of the individuals to whom the data relates. In view of the relevant situation, the Company also ensures that the frequency of internal audits is increased in terms of the compliance of personal data processing with the law, as well as the verification and updating of data in the database in order to ensure the continued compliance of processed data with the facts.

After reviewing the whole of the evidence gathered in the case, the President of the PDPO considered the following.

The President of the PDPO, when issuing an administrative decision, is obliged to decide based on the facts existing at the time of issuing the decision. As the doctrine states, "the public administration authority evaluates the factual state of the case according to the moment of issuing the administrative decision. This rule also applies to the assessment of the legal state of the case, which means that the public administration authority issues an administrative decision on the basis of the law in effect at the time of its issuance (...). Adjudication in administrative proceedings involves applying the applicable law to the established facts of an administrative case. Thus, the public administration authority realizes the purpose of administrative proceedings, which is the realization of the applicable legal norm in the field of administrative-legal relations, when these relations require it" (Commentary to the Act of 14 June 1960, Code of Administrative Procedure M. Jaskowska, A. Wróbel, Lex., el/2012).

Pursuant to Article 17(1) of the GDPR the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay, inter alia if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (Art(1)(a) of the GDPR), if 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 (Art. 17 (1)(b) of the GDPR) or also if the personal data have been unlawfully processed (Art. 17(1)(d) of the GDPR).

However, pursuant to Article 12(2) of the GDPR 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.

Moreover, 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 (Article 12(3) of the GDPR).

In the course of the administrative proceedings, it was established that on 7 September 2021 the Complainant requested the Company via an email to delete her personal data, including the account established in the service available on the website

[REDACTED] 14 September 2021 the Complainant again requested the same thing from the Company through another email sent to the Company. As of the date of the Complainant's complaint, i.e. 14 November 2021 the Complainant was still able to access the website in question using her credentials, and her request for deletion by the Company had not been processed. The Company, in its explanations, admitted that due to a technical error involving the misclassification of messages by the email server, the messages with the Complainant's request were moved to the SPAM folder, as a result of which there was a delay in the processing of the request for deletion of the Complainant's data, and the data was not deleted until 19 May 2021, of which the Company informed the Complainant via email on the same day (evidence: two screenshots responding to the Complainant's requests of September 7 and 14, 2021). It should also be pointed out that despite the lack of expediency in the Company's actions, the Company did not act promptly, or at the latest within a month, on the Complainant's request to delete her data in accordance with its obligation under the provisions of the GDPR as a controller.

As indicated in Recital 59 of the GDPR, modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

In the light of the above, it should be pointed out that the Company has failed to comply with the disposition specified in Article 12(3) of the GDPR. It is clear from the evidence gathered in the case that the Complainant requested the deletion of her data twice, including for the first time on 7 September 2021, while the Company deleted the

Complainant's data only after the intervention of the President of the PDPO on 19 May 2022, thus definitely after the deadlines under Article 17(1) of the GDPR and informed the Complainant of this in violation of the deadline under Article 12(3) of the GDPR. Accordingly, the President of the PDPO, pursuant to Article 58(2)(b) of the GDPR, provided a reprimand to the Company in this regard.

The President of the PDPO, acting on the basis and within the limits of the powers granted to him by the provisions of the GDPR, when issuing a decision examines the factual and legal situation as of the date of the decision. In the present case, the Company failed to comply with its obligations as an controller and violated the provisions of Articles 12(3) and 17(1) of the GDPR. Accordingly, the President of the PDPO has decided to provide a reprimand to restore compliance with the law. Referring to the regulation of Article 58(2)(c) of the GDPR, it should be noted that the President of the PDPO may order a controller or processor to comply with a data subject's request arising from his or her rights under the regulation, i.e. to restore the state of lawfulness in the event of a violation of data protection regulations. However, the fundamental fact affecting the content of this ruling is that the Complainant's request for deletion of personal data was finally granted by the Company and the Complainant's personal data is not currently being processed in the disputed manner, so the authority cannot order its deletion.

In this factual and legal state, the President of the PDPO has adjudicated as indicated in the operative part of the decision.

**Under the authority of the
President of the Personal Data Protection Office
Director of the Complaints Department**



The decision is final. Pursuant to Article 7(2) of the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws 2019, item 1781) in connection with Article 13 § 2, Article 53 § 1 and Article 54 § 1 of the Act of 30 August 30 2002 Law on Procedure before Administrative Courts (Journal of Laws 2022, item 329, as amended), the party has the right to lodge a complaint against this decision with the Voivodeship Administrative Court in Warsaw, within 30 days from the date of its delivery to the party. The complaint is lodged via the President of the Personal Data Protection Office. The fee for the complaint is in the amount of 200 PLN. The party has the right to apply for the right of aid, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of aid may be granted upon the request of a party submitted before the initiation of the procedure or in the course of the procedure. This request is free of court fees.

**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**

Jan Nowak

Warsaw, 16th January 2023

DS.523.2942.2020.ZS.BS

DECISION

On the basis of Article 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2022 item 2000 as amended) and Article 7 (1) of the Act of 10 May 2018 on the personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781) and on the basis of Article 60 (6) and (8) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1, OJ L 127, 23.5.2018, p. 2 and OJ L 74, 4.3.2021, p. 35), after carrying out the administrative proceedings regarding the complaint of [REDACTED]

[REDACTED] residing in Wrocław at [REDACTED] represented by legal advisor [REDACTED] from [REDACTED] law firm based in Wrocław at [REDACTED], relating to irregularities in the processing of [REDACTED]
[REDACTED] s residing in Wrocław at [REDACTED], personal data by [REDACTED]
[REDACTED] based in Munich at [REDACTED] consisting in failure to comply with the information obligation in accordance with Article 15 of the above-mentioned Regulation, the President of the Personal Data Protection Office

dismisses the complaint.

JUSTIFICATION

The Personal Data Protection Office has received a complaint of [REDACTED]
[REDACTED] residing in Wrocław at [REDACTED], hereinafter: the Complainant, represented by legal advisor [REDACTED] law firm based in Wrocław at [REDACTED] relating to irregularities in the processing of the Complainant's personal data by [REDACTED] based in Munich at [REDACTED] consisting in failure to comply with the information obligation in accordance with Article 15 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1, OJ L 127, 23.5.2018, p. 2 and OJ L 74, 4.3.2021, p. 35), hereinafter: the Regulation 2016/679.

According to Article 55 (1) of the Regulation 2016/679, each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State. Moreover, Article 56 (1) states that without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the

cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

The President of the Personal Data Protection Office, hereinafter also referred to as the President of the UODO, identified the case as having a cross-border nature in accordance with Article 4 point 23 of the Regulation 2016/679 and therefore handled the case over to the German supervisory authority competent for the federal state of Bavaria (German: *Bayerisches Landesamt für Datenschutzaufsicht*), hereinafter referred to as: BayLDA. Due to the fact that the main establishment of the Company is located in the territory of the federal state of Bavaria, the consideration of the case in question, due to the cross-border nature of the complaint, was within the exclusive jurisdiction of BayLDA, which accepted the case as the lead supervisory authority 26th February 2021.

In the course of administrative proceedings, the President of the Personal Data Protection Office established the following facts:

1. The complaint was originally directed against [REDACTED] [REDACTED] with its registered office in Warsaw at [REDACTED] [REDACTED] hereinafter referred to as: [REDACTED] The Complainant complained about the failure to receive the police report on the accident that took place on 15th October 2019 in the territory of the Federal Republic of Germany and claimed that there had been a violation of Article 6 (1)(f) and Article 15 (1) of the Regulation 2016/679 (proof: complaint of 27th May 2020; BayLDA draft decision of 6th October 2022).
2. The President of the UODO asked [REDACTED] S.A. for explanations regarding the facts of the case. Based on the explanations received on 20th August 2020, it was established that the data controller in connection with the processing challenged in the complaint is [REDACTED] with its registered office in Munich at [REDACTED] hereinafter referred to as: the Company (proof: complaint of 27th May 2020; explanations of [REDACTED] dated 20th August 2020; BayLDA draft decision of 6th October 2022).
3. The insurance case under consideration for the processing process challenged in the complaint concerns a motor vehicle liability claim that occurred on 15th October 2019 as a result of a traffic accident on the A4 motorway in Germany. The driver of the policyholder's vehicle crashed into the Complainant vehicle. At the time of the accident, apart from the Complainant, there were two other people in the vehicle, all three of the victims are Polish citizens and live in Poland (proof: complaint of 27th May 2020; explanations of the Company of 7th June 2021).
4. The Company confirmed the existence of a compulsory third party liability insurance contract concluded with the policyholder of German citizenship (the perpetrator of the accident). The insurance covers the operation of his vehicle under German license plates by him as a driver and keeper, as well as by other drivers who are also insured (proof: explanations of the Company of 7th June 2021).
5. The Company has established the sole liability of the driver of the vehicle covered by the insurance provided by the Company. Police records in criminal proceedings

against the driver of the policyholder's vehicle were also used to assess liability and insurance risk. For this purpose, the Company applied for access to the files to the competent investigative authority as part of legal representation in relation to the insurance contract, as a civil liability insurer (proof: explanations of the Company of 7th June 2021).

6. The Complainant applied to [REDACTED] as the Company's representative for claims, for the payment of compensation for the harm suffered (proof: complaint of 27th May 2020).
7. The Complainant was covered by the additional [REDACTED], therefore he also reported the damage to [REDACTED] with its registered office in Warsaw, hereinafter referred to as: [REDACTED] in order to obtain compensation. In order to carry out the liquidation of the damage, [REDACTED] asked the Complainant to present the documentation of the accident, including the police report on the accident, under pain of refusal to pay the benefit (proof: complaint of 27th May 2020).
8. In February 2020, the Complainant, through [REDACTED] asked the Company to provide the police report on the accident in order to present it to [REDACTED] for the purpose of liquidating the damage. The company replied to [REDACTED] that, for legal reasons arising from German criminal law, it was not possible to make the investigation files available to the Complainant. In the letter of 24th February 2020, [REDACTED] informed that the Company did not consent to the disclosure of the police note due to the protection of personal data (proof: complaint of 27th May 2020; letter of [REDACTED] to the Complainant of 24th February 2020 ; explanations of the Company of 7th June 2021).
9. On 14th May 2021, the Company sent a letter to the Complainant with information on the processing of his personal data. The company confirmed that it processes the Complainant's personal data. In addition, the Company provided the Complainant with information about: stored data (along with a list of stored data), processing purposes, recipients or categories of data recipients, the period of personal data storage, the rights of the data subject and the right to lodge a complaint with the supervisory authority and the origin of the data, provided that they have not been collected from the data subject (proof: explanations of the Company of 21st June 2021).

After reviewing the collected evidence, the President of the Personal Data Protection Office considered the following.

According to the wording of Article 60 (3) of the Regulation 2016/679, 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. 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, i.e., respectively, four weeks for a draft decision or two weeks for a revised draft decision, 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 (Article 60 (6) of the Regulation 2016/679).

As a rule, 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 European Data Protection Board of the decision in question, including a summary of the relevant facts and grounds, while the supervisory authority with which a complaint has been lodged shall inform the complainant on the decision (Article 60 (7) of the Regulation 2016/679). However, in accordance with Article 60 (8) of the Regulation 2016/679, by derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

BayLDA, after conducting the proceedings regarding the submitted complaint, acting pursuant to Article 60 (3) of the Regulation 2016/679, on 14th October 2022, submitted a draft decision of 6th October 2022, to the other supervisory authorities concerned, including the President of the Personal Data Protection Office, for their opinion and take due account of their views. Within the four-week period referred to in Article 60 (4) of the Regulation 2016/679, none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority.

The President of the Personal Data Protection Office, as the supervisory authority concerned, is therefore bound by the draft decision of BayLDA of 6th October 2022 pursuant to Article 60 (6) of the Regulation 2016/679. Due to the agreement reached by the lead supervisory authority and the supervisory authorities concerned that the complaint should be dismissed, in accordance with the disposition of Article 60 (8) of the Regulation 2016/679, the President of the Personal Data Protection Office, as the supervisory authority with which a complaint has been lodged, adopts this decision and notifies it to the Complainant and informs the Company (data controller) thereof.

Considering the above, the President of the Personal Data Protection Office agreed with the decision, factual findings and legal justification presented by BayLDA in the draft decision of 6th October 2022 and accepted them as his own.

When issuing an administrative decision, the President of the Personal Data Protection Office is obliged to settle the case based on the facts existing at the time of issuing the decision. As stated in the doctrine, "the public administration authority assesses the facts of the case at the time of issuing the administrative decision. This rule also applies to the assessment of the legal status of the case, which means that the public administration body issues an administrative decision on the basis of the provisions of law in force at the time of its issuance (...). Settling in administrative proceedings consists in applying the applicable law to the established facts of the administrative case. In this way, the public administration body achieves the goal of administrative proceedings, which is the implementation of the applicable legal norm in the field of administrative and legal relations, when these relations require it" (Commentary to the Act of 14 June 1960, Code of Administrative Procedure M. Jaśkowska, A. Wróbel, Lex., el/2012). At the same time, this authority shares the position expressed by the Supreme Administrative Court [Naczelnego Sądu Administracyjnego] in the

judgment of 25th November 2013, issued in the case with reference number I OPS 6/1, in which the above-mentioned Court indicated as follows: "In administrative proceedings, regulated by the provisions of the Code of Administrative Procedure, the rule is that the public administration body settles the case by issuing a decision that settles the case as to its essence, according to the legal and factual status as at the date of the decision".

First of all, it should be pointed out that the administrative proceedings conducted by the President of the UODO are to control the compliance of data processing with the provisions on the protection of personal data and are aimed at restoring the lawful state by issuing an administrative decision pursuant to Article 58 (2) of the Regulation 2016/679.

In the judgment of 7th May 2008 in the case with reference number I OSK 761/07, the Supreme Administrative Court [Naczelnny Sąd Administracyjny] stated that "when examining [...] the lawfulness of personal data processing, GIODO is obliged to determine whether, as of the date of issuing a decision in the case, the data of a specific entity is processed and whether it is done in a lawful manner".

Pursuant to Article 15 (1) of the Regulation 2016/679, 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.

Article 15 (3) of the Regulation 2016/679 states, that 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.

The collected evidence shows that in February 2020, the Complainant, through ██████████ asked the Company to provide a police note from the accident, which was supposed to contain his personal data, in order to present it to █████ for the purpose of liquidating the damage. However, the evidence does not show that the Complainant requested the Company to provide information pursuant to Article 15 (1) of the Regulation 2016/679. Request to fulfill the information obligation towards the Complainant by indicating: what personal data concerning the Complainant were

processed, what were the purposes of processing, how long the data will be stored and to which recipients the Complainant's data have been or will be disclosed, and request to provide the Complainant with a copy of his personal data subject to processing, were formulated only in the letter of the Complainant's attorney of 31st July 2020, addressed to the President of the UODO. Therefore, it should be assumed that the Company received the above-mentioned requests together with the letter of BayLDA dated 21st April 2021 addressed to the Company.

According to Article 12 (3) of the Regulation 2016/679 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 collected evidence clearly shows that the Company responded to the Complainant's request for access to the processed data within the prescribed period and provided him with a copy of his personal data subject to processing. The Company submitted proof of the fact that on 14th May 2021 it provided the Complainant with information pursuant to Article 15 (1) of the Regulation 2016/679 and provided him with a copy of his personal data subject to processing, as requested by the Complainant's attorney in the letter of 31st July 2020, addressed to the President of the UODO, which was received by the Company on 21st April 2021. With regard to the above, the authority states that the Complainant's allegations are not supported by the evidence, because the Company has presented evidence for the timely and reliable fulfillment of the controller's obligations and exercising the Complainant's right to obtain information pursuant to Article 15 (1) of the Regulation 2016/679 and provided the Complainant with a copy of the personal data subject to processing in accordance with Article 15 (3) of the Regulation 2016/679.

Referring to the Complainant's allegation regarding the Company's refusal to provide a copy of the police note from the accident involving the Complainant, which took place on 15th October 2019 in Germany, BayLDA in the draft decision of 6th October 2022, followed by the President of the Personal Data Protection Office, being bound by the content of the draft decision pursuant to Article 60 (6) of the Regulation 2016/679, determined that the Complainant's request in this respect is manifestly unfounded.

The right to request access to personal data by the data subject is not unconditional. According to Article 15 (4) of the Regulation 2016/679, the right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others. On the other hand, the Article 12 (5) of the Regulation 2016/679 states that where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may, among others, refuse to act on the request.

The police note from the accident involving the Complainant, which took place on 15th October 2019 in Germany, is part of the police files, in relation to which the issue of access to documents is regulated by the provisions of German criminal procedure law. The right of access to the file is granted only within the narrow limits laid down in the provisions of the German Code of Criminal Procedure (StPO), expressly defined for this purpose by the German legislator and not against the insurance company, but against the competent investigating authority. The Company requested access to the file, taking

advantage of its subjective legal position as an insurer, which is an “other entity” under Article 475 of the German Code of Criminal Procedure (StPO). The investigating authority, recognizing the Company’s procedural rights, allowed the Company to exercise its right of access to files.

According to Article 32f (5) of the German Code of Criminal Procedure (StPO), persons who have been granted access to files are prohibited from distributing files, documents, printouts or copies obtained from them, passing them on to third parties for non-procedural purposes or otherwise making them available.

Pursuant to Article 23 (1)(d) of the Regulation 2016/679, Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard, among others, the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Considering the above, the authority concluded that pursuant to Article 23 (1)(d) of the Regulation 2016/679, the provision of Article 32f (5) of the German Code of Criminal Procedure (StPO) constitutes a lawful limitation of the scope of the obligations and rights provided for in Article 15 of the Regulation 2016/679. The Company was under an obligation to refuse to provide the Complainant with a copy of the police report of the accident, as otherwise it would be subject to criminal liability for a violation of Article 32f (5) of the German Code of Criminal Procedure (StPO).

Just as an aside, the authority notes that the Complainant, who is granted the status of a victim of the accident under investigation by the provisions of the German Code of Criminal Procedure (StPO), should be entitled to access police files. However, the request for access to the files should be addressed to the investigating authority conducting the proceedings, and not – as was in this case – to the insurer (the Company).

Administrative proceedings conducted by the President of the Personal Data Protection Office are to control the compliance of data processing with the provisions on the protection of personal data and are aimed at issuing an administrative decision pursuant to Article 58 of the Regulation 2016/679, on the basis of which the supervisory authority may restore the lawful state. In the case in question, it was established that there was no violation of the Complainant’s rights under Article 15 (1) and (3) of the Regulation 2016/679. The Company responded to his request within the deadlines, and thus the allegation made by the Complainant against the Company was not confirmed. In addition, the Company, in accordance with Article 12 (5)(b) of the Regulation 2016/679, reasonably refused to take action in connection with the Complainant’s request to provide a copy of the police note from the accident, due to its manifestly unfounded nature, having regard the compliant with Article 23 (1)(d) of the Regulation 2016/679 limitation of the scope of obligations and rights provided for in Article 15 of the Regulation

2016/679 resulting from the provision of Article 32f (5) of the German Code of Criminal Procedure (StPO). In view of the above, there are no grounds for applying corrective measures aimed at restoring the lawful state. Considering the above, the President of the Personal Data Protection Office decided to dismiss the complaint.

In this factual and legal state, the President of the Personal Data Protection Office decided as in the sentence.

Under the authority of the President
of the Personal Data Protection Office
the Head of the Complaints Department



The decision is final. Based on Article 7 (2) of the Act of 10 May 2018 on the personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2022, item 329, as amended), the party has the right to lodge a complaint against this decision to the Provincial Administrative Court in Warsaw [Wojewódzki Sąd Administracyjny w Warszawie], within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warsaw). The court fee for a complaint is PLN 200. The party has the right to apply for the right of assistance.



**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**
Jan Nowak

Warsaw, 23 March, 2020

ZSPR.440.1959.2019.PT.MKA

(Previous case number ZSPR.440.1959.2019.ZS.MKA)

DECISION

Pursuant to Article 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws 2020, item 256, as amended), Article 5(1)(b), Article 6(1), Article 17(1)(a), Article 58(2)(c) and Article 60(7) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Journal of Laws EU L 119 of 04.05.2016, p. 1 and Journal of Laws of the EU L 127 of 23.05.2018, p. 2), having conducted an administrative procedure in the case of complaint of [REDACTED], residing in [REDACTED]
[REDACTED] regarding the irregularities in the processing of his personal data by [REDACTED]
[REDACTED] with its seat in [REDACTED], consisting in not complying
with a request to erase the personal data of [REDACTED], the President of the Personal
Data Protection Office,

orders [REDACTED] to erase the
personal data of [REDACTED]
[REDACTED], in the scope of: name, surname, PESEL number, mother's family
name, parents' names, date of birth, gender, country of birth, place of birth, residence
status, tax status, citizenship, residence address, correspondence address, e-mail
address, series and number of identification document "dowód osobisty", passport
number, mobile phone number, marital status, housing status, education, number of
people in the household, costs of the household, source of income, period of acquiring
income, employer's data, active profession, amount of income.

Substantiation

Complaint has been lodged with the President of the Personal Data Protection Office [hereinafter: the President of the Office] by [REDACTED], residing in [REDACTED]
[REDACTED] [hereinafter: the Complainant] regarding the irregularities in the processing of his personal data by [REDACTED]
[REDACTED] [hereinafter: the Bank], consisting in not complying with a request to erase the personal data of the Complainant.

In the complaint the Complainant requested the erasure of all his personal data by the Bank.

In the course of the procedure the President of the Personal Data Protection Office has established the following factual state.

1. The Bank has indicated that it has obtained the personal data of the Complainant directly from him, in connection with the conclusion of agreements of 23 September 2013, including a framework agreement for the usage of an internet banking system as well as an account agreement, agreement for a payment card to the account and the agreement for the usage of an electronic banking system for individual clients. (evidence: letter of the Bank of 13 March 2020 with attachments)
2. In connection with the conclusion and execution of the agreements the Bank has obtained the data of the Complainant in the scope of: name, surname, PESEL number, mother's family name, parents' names, date of birth, gender, country of birth, place of birth, residence status, tax status, citizenship, residence address, correspondence address, e-mail address, series and number of identification document "dowód osobisty", passport number, mobile phone number, marital status, housing status, education, number of people in the household, costs of the household, source of income, period of acquiring income, employer's data, active profession, amount of income. (evidence: letter of the Bank of 13 March 2020 with attachments)
3. In October 2018 the Complainant has issued a disposition to close all the bank accounts and to terminate all the agreements which he entered into with the Bank (evidence: request of the Complainant of 4 August 2019)
4. On 26 and 27 July 2019, the Complainant received e-mail messages, which according to him were of marketing nature and in connection with the messages received, the

Complainant requested the Bank to erase his data and discontinue the processing of data for marketing purposes (evidence: the Complainant's request of 4 August 2019)

5. The complainant has issued a request to erase his personal data and to discontinue the processing of his data for marketing purposes on 12 September 2019 (evidence: the Bank's letter of 13 March 2020 with attachments)
6. The e-mail correspondence sent to the Complainant on 26 July 2019 wasn't of marketing nature, but only constituted informational communication related to the change in the method of providing the obligatory reports (daily transaction confirmations and quarterly brokerage account statements). (evidence: the Bank's letter of 13 March 2020 with attachments)
7. On 16 September 2019 the Bank has replied to the Complainant's requests, indicating that it is discontinuing the processing of his personal data for marketing purposes. In addition, he was informed about the closure of the [REDACTED] service and was assured that the data will be processed only for archival purposes. (evidence: the Bank's letter of 13 March 2020 with attachments)
8. The Bank, after it has received the Complainant's complaint, analyzed the response sent to the Complainant on 16 September 2019 and found that its reply was incomplete. The Bank did not provide the Complainant with information on data processing in connection with the "Agreement for the provision of services of accepting and transferring orders for acquisition and re-acquisition of participation titles in collective investment institutions" of 29 June 2016. The above irregularity was the result of an employee's error who has not verified that the client possessed the abovementioned agreement and has not closed it. As a consequence, the Complainant received incorrect information that his data was processed only for archival purposes. In connection with the wrongful compliance with the Complainant's request for the erasure of personal data, the Bank undertook corrective measures: • sent a letter to the Complainant with rectification of information regarding the processing of his personal data; • on 3 March 2020 it has closed the "Agreement for the provision of services of accepting and transferring orders for acquisition and re-acquisition of participation titles in collective investment institutions" • took out consequences against the employee who provided incorrect information regarding the processing of the Complainant's data; • introduced a "checklist of the employee's actions while handling the client's request", which aims to minimize the likelihood of such errors in the future; • scheduled a training for employees responsible for answering clients in the scope of personal data.

9. Currently, the Bank processes the obtained Complainant's personal data for archival purposes. The Complainant's personal data will be processed for a period of 10 years from the date of termination of the "Agreement for the account "Open Savings Account Bonus" of 31 December 2017, which was terminated on 30 April 2018 (this is the period for agreements terminated before 9 July 2018). However, for agreements terminated after 9 July 2020 personal data will be processed for a period of 6 years from the date of termination of the agreement. The legal basis for the processing of data for the indicated periods is Article 118 of the Act of 23 April 1964 Civil Code (hereinafter: the Civil Code). These periods differ due to the Act amending the Civil Code (Act of 13 April 2018 on amending the Civil Code and certain other acts) which entered into force on 9 July 2018 and modified the limitation period for claims (proof: Bank's letter of March 13, 2020 with attachments)

After getting acquainted with the collected evidence, the President of the Office has considered the following.

The President of the Office, when issuing an administrative decision, is obliged to adjudicate based on the factual state at the time of the decision. As indicated in the doctrine, "the public administration body assesses the factual state of the case according to the moment of issuing the administrative decision. This rule also applies to the assessment of the legal state of the case, which means that the public administration authority issues an administrative decision on the basis of the provisions of law in force at the time of its issuance (...). Adjudication in administrative procedures consists in applying the law in force to the established factual state of an administrative case. In this way, the public administration body realizes the purpose of administrative procedures, which is the implementation of the binding legal norm in the field of administrative-legal relations, when such relations require it" (Commentary to the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws 00.98.1071) M. Jaśkowska, A. Wróbel, Lex., el/2012). Furthermore, in the judgment of 7 May 2008 in the case with reference number I OSK 761/07 The Supreme Administrative Court stated that "when examining the legality of the processing of personal data, GIODO is obliged to determine whether the data of a specific entity are processed on the date of adjudicating the case and whether it is conducted in accordance with the law".

Firstly, it should be indicated that 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), (Journal of Laws EU L 119 of 04.05.2016, p. 1

and Journal of Laws of the EU L 127 of 23.05.2018, p. 2) [hereinafter: GDPR] determines the lawfulness of processing of personal data. Each of the conditions in Article 6(1) of the GDPR is autonomous and independent, which means that the fulfillment of one of them in a given case confirms the lawfulness of the processing of personal data. Furthermore, it should also be emphasized that the consent of the data subject is not the only basis legalizing the processing of its personal data (point a). The data processing will be compliant with the provisions of the act also when the data controller demonstrates that at least one condition of the aforementioned Article 6(1) of the GPDR is met. This provision states that the processing is lawful, when, among others: 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 (Article 6(1)(b)); processing is necessary for compliance with a legal obligation to which the controller is subject (Article 6(1)(b)); 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 (Article 6(1)(f)).

Pursuant to Article 5(1)(b) of the GDPR, personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Until the Complainant has issued a disposition to terminate all agreements between him and the Bank in October 2018, while processing the Complainant's personal data the Bank had the legal basis for the processing in accordance with Article 6(1)(b) of the GDPR.

After issuing the disposition to terminate all agreements between the Complainant and the Bank and in connection with the request to erase all his personal data of 12 September 2019, in the opinion of the President of the Office, the processing of the Complainant's personal data by the Bank in the scope of name, surname, PESEL number, mother's family name, parents' names, date of birth, gender, country of birth, place of birth, residence status, tax status, citizenship, residence address, correspondence address, e-mail address, series and number of identification document "dowód osobisty", passport number, mobile phone number, marital status, housing status, education, number of people in the household, costs of the household, source of income, period of acquiring income, employer's data, active profession, amount of income, has not been legally substantiated by the provisions of the GDPR. Further processing of the Complainant's personal data by the Bank constitutes a breach of Article 6(1) and 17(1) of the GDPR. According to Article 17(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 including if

the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

The Bank indicated that it is currently processing the Complainant's data for archiving purposes, but has in no way demonstrated the circumstances justifying the processing after the Complainant has closed all the agreements. Moreover, the Bank indicated that the legal basis for data processing period is Article 118 of the Civil Code.

The period of storage of the Complainant's personal data was determined in relation to the protection against potential claims of the Complainant, it must be stated that the evidence collected in this case did not show that the Complainant has raised any claims against the Bank which would justify the Bank's right to store and process his personal data for evidence purposes in relation to the Complainant's exercise of his claim. Therefore, In the opinion of the President of the Office, the condition of necessity for the purposes of the legitimate interests pursued by the controller with regard to the processing of the Complainant's personal data has not been fulfilled.

The condition of Article 6(1)(f) of the GDPR applies to an already existing situation in which the purpose resulting from the legitimate interests pursued by the controller is the necessity to prove, the necessity to exercise or to defend against an existing claim, and not a situation in which data is processed in order to protect against a potential claim. Since the administrative procedure conducted by the President of the Office has not shown that the Complainant raised any claims against the Bank, it must be stated that the Bank processes the Complainant's personal data in the abovementioned purpose for the purpose only "in case of", in order to protect against potential and uncertain claims of the Complainant. The President of the Office also agrees with the position of the Voivodeship Administrative Court in Warsaw regarding the condition analogous to the condition of Article 6(1)(f) of the GDPR, namely the condition resulting from Article 23(1)(5) of the Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws of 2016, item 922, as amended), regarding the legality of processing personal data necessary for the legally justified purposes carried out by data controllers or data recipients, when the processing does not violate the rights and freedom of the data subject. The court in its judgment of 1 December 2010 in the case with reference number II SA/Wa 1212/10 (LEX no. 755113) ruled, quote: "In the present case, the authority argued that the complainant had raised objections to the company regarding the legality of the processing of his data and announced the intent to bring the case before the court. Hence, the company was entitled to record the complainant's data and keep them for evidence purposes in the event that the complainant exercised any claims. In the opinion of the Court, the above

circumstances do not meet the condition of legally justified purposes for processing of the complainant's data. It should be noted that the condition of Art. 23(1)(5) of the act applies to an already existing and certain situation, i.e. when there is a necessity to prove, the necessity to exercise a claim related to business activity, and not a situation where data is processed in the event of a potential procedure and a potential necessity to prove that the personal data obtained without the consent of the data subject are processed in accordance with the law. Therefore, in the opinion of the Court, the company cannot process the complainant's personal data only in order to protect itself against a potential future and uncertain claim of the complainant. Otherwise, there may be doubt regarding how long the complainant's personal data should be processed if he fails to fulfill his announced intention".

It should be emphasized that if the abovementioned provisions were interpreted differently, the Complainant would be deprived of protection under the GDPR and the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws 2019, item 1781). It must be stated that accepting the position that the processing of personal data in order to avoid negative consequences in the event of raising a potential and undefined claim in the future is a legitimate interest within the meaning of Article 6(1)(f) of the GDPR as correct, would mean that the Complainant's personal data may be processed by the Bank permanently, without the necessity to erase them. It is theoretically possible for the Complainant to raise a claim with the Bank after the limitation period for the claim has expired. This would lead to the conclusion that the processing of the Complainant's personal data by the Bank is justified by the condition of Article 6(1)(f) of the GDPR for the purpose of exercising the right to defense against a potential claim of the Complainant also after the expiry of the abovementioned period.

At this point, it must be indicated that there is no justification in assuming that periods for the limitation of claims arising from the obligations also define the periods in which personal data may be processed by the Bank. It is necessary to indicate that the limitation period for a claim does not have effects in the field of protection of personal data, as it does not affect the existence of the claim, but only affects the field of procedural charges in the form of the possibility of raising the limitation of claims in a court dispute. It should be emphasized that the circumstance justifying the processing of personal data for the purpose of exercising claims is the very fact of the existence of a claim and the intention to exercise it, but not a change in the procedural rights of the defendant entity.

It must be stated that a public administration body may consider the factual state of the case as established only on the basis of undoubtable evidence and in this respect, it cannot limit itself to making what is probable - unless the provisions of the Act of 14 June 1960 Code of

Administrative Procedure (Journal of Laws 2020, item 256, as amended) (hereinafter: Code of Administrative Procedure) provide otherwise (e.g. Article 24 of the Code of Administrative Procedure). As indicated by the Supreme Administrative Court in the judgment of 9 July 1999 (III SA 5417/98), "the authority conducting the procedure must seek to establish the material truth and, according to its knowledge, experience and internal reasoning, assess the evidential value of individual evidence, the impact of proving one circumstance on other circumstances". In the same judgment, the Court also stated that there is a rule in an administrative procedure that the burden of evidence lies with the person who derives legal consequences from a specific fact.

Therefore, there are grounds to apply the provision of Article 58(2)(c) of the GDPR. Pursuant to this provision, in the event of a breach of the provisions on the protection of personal data, the President of the Office orders the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to the GDPR. Therefore, the obligatory condition has been met for the President of the Office to issue a decision ordering the erasure of the Complainant's personal data in the scope of his name, surname, PESEL number, mother's family name, parents' names, date of birth, gender, country of birth, place of birth, residence status, tax status, citizenship, residence address, correspondence address, e-mail address, series and number of identification document "dowód osobisty", passport number, mobile phone number, marital status, housing status, education, number of people in the household, costs of the household, source of income, period of acquiring income, employer's data, active profession, amount of income.

In this factual and legal state, the President of the Personal Data Protection Office has adjudicated as indicated in the operative part of the decision.

**Under the authority of the President
of the Personal Data Protection Office**



The decision is final. Pursuant to Article 7(2) of the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws 2019, item 1781) in connection with Article 13 § 2, Article 53 § 1 and Article 54 § 1 of the Act of 30 August 30 2002 Law on Procedure before Administrative Courts (Journal of Laws 2018, item 1302, as amended), the party has the right to lodge a complaint against this decision with the Voivodeship Administrative Court in Warsaw, within 30 days from the date of its delivery to the party. The complaint is lodged via the President of the Personal Data Protection Office. The fee for the complaint

is in the amount of 200 PLN. The party has the right to apply for the right of aid, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of aid may be granted upon the request of a party submitted before the initiation of the procedure or in the course of the procedure. This request is free of court fees.

TRANSLATION

PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE

Jan Nowak

Warsaw, 29 April 2021

Ref. No.: ZSPR.440.464.2019.PT.BS

(previous Ref. No.: ZSPR.440.464.2019.ZS.AS)

DECISION

On the basis of Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2020 item 256, as amended) and Article 7 para. 1 of the Act of 10 May 2018 on the personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781), the President of the Personal Data Protection Office in the case of [REDACTED], residing at [REDACTED]), relating to irregularities in the processing of his personal data by [REDACTED] with its registered seat in Luxembourg, [REDACTED]), consisting in not fulfilling the request to erase the personal data of [REDACTED],

decides to discontinue the proceedings.

JUSTIFICATION

On 14 February 2019, the Personal Data Protection Office received a complaint from [REDACTED] [REDACTED], residing at [REDACTED], hereinafter referred to as: ‘the Complainant’, on irregularities in the processing of his personal data by [REDACTED] based in Luxembourg with its seat in Luxembourg at [REDACTED] hereinafter referred to as the Company, consisting in failure to comply with the request to erase Complainant’s personal data.

On 27 August 2020, the Personal Data Protection Office received a letter from the Complainant informing that he withdraws the complaint submitted to the President of the Personal Data Protection Office.

Due to the withdrawal of the complaint, the proceedings became redundant, and the present proceedings are subject to discontinuation pursuant to Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2020 item 256, as amended), hereinafter referred to as: ‘the Code of Administrative Procedure’. In accordance with the above-mentioned provision, when the proceedings for any reason have become redundant in whole or in part, the public administration authority shall issue a decision to discontinue the proceedings, in whole or in part, respectively. The wording of the above-mentioned provision leaves no doubt that in the event when the proceedings are deemed groundless, the authority conducting the proceedings obligatorily discontinues them.

The determination by the public authority of the existence of the premise referred to in Article 105 § 1 of the Code of Administrative Procedure obliges it, as it is emphasized in the doctrine and jurisprudence, to discontinue the proceedings.

In this factual and legal background, the President of the Personal Data Protection Office adjudicated as in the operative part.

Under the authority of the President
of the Personal Data Protection Office



This decision is a final decision. Based on Article 7 para. 2 of the Act of 10 May 2018 on the Protection of Personal Data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2019, item 2325), the party has the right to bring a complaint to the Wojewódzki Sąd Administracyjny w Warszawie [Voivodeship Administrative Court in Warsaw] against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of assistance may be granted upon application by a party submitted prior to the initiation of the proceedings or in the course of the proceedings. This application is exempt from court fees.

**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**
Jan Nowak

Warsaw, 8th June 2021

Ref. No.: ZSPR.440.1114.2019.PT.BS
(previous Ref. No.: ZSPR.440.1114.2019.ZS.LS)

DECISION

On the basis of Article 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021, item 735) and Article 6 para. 1, Article 12 para. 3 in connection with Article 15, Article 15 para. 1 and Article 58 para. 2 letter b) and c) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), after having carried administrative proceedings in the case of ██████████, residing at ██████████ in Tallinn, relating to irregularities in the processing of his personal data and failure to respond to the request for access to data, within the time limit provided for in Article 12 para. 3 of the Regulation mentioned above, by ██████████ with its headquarters in Warsaw at ██████████, the President of the Personal Data Protection Office

- 1) issues a reprimand to ██████████ with its headquarters in Warsaw at ██████████ for violation of Article 6 para. 1 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2, and OJ EU L 74 of 04/03/2021, p. 35), for the processing of ██████████, residing at ██████████ in Tallinn, personal data in the form of information about his citizenship, date of birth, number and expiry date of his identity card without legal basis;
- 2) issues a reprimand to ██████████ with its headquarters in Warsaw at ██████████ for violation of Article 12 para. 3 in connection with Article

15 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), consisting in failure to respond to the request of [REDACTED], residing at [REDACTED] in Tallinn, within the time limit prescribed in Article 12 para. 3 of the mentioned above Regulation;

- 3) orders [REDACTED]. with its headquarters in Warsaw at [REDACTED] to grant [REDACTED], residing at [REDACTED] in Tallinn, access to the scope of his personal data which it holds.

JUSTIFICATION

The Personal Data Protection Office received a complaint from [REDACTED], residing at [REDACTED] in Tallinn, hereinafter referred to as: the Complainant, about irregularities in the processing of his personal data and the failure to respond to the request for access to data within the time limit provided for in Article 12 para. 3 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), hereinafter referred to as: Regulation 2016/679, by [REDACTED] with its headquarters in Warsaw at [REDACTED], hereinafter referred to as: the Company. The complaint was provided by the Estonian supervisory authority (Andmekaitse Inspektsioon) to the President of the Personal Data Protection Office as a lead supervisory authority pursuant to Article 56 para. 1 of Regulation 2016/679, through the Internal Market Information System established by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC (OJ EU L 316 of 04/11/2012, p. 1) in connection with the Commission Implementing Decision (EU) 2018/743 of 16 May 2018 on a pilot project to implement the administrative cooperation provisions set out in Regulation (EU) 2016/679 of the European Parliament and of the Council by means of the Internal Market Information System (OJ EU L 123 of 18/05/2018, p. 115).

The Complainant pointed out that the Company did not respond to his request for access to data, which included information on the reasons why, before boarding the aircraft operated by the

Company, he had been asked to provide additional data (apart from those collected from him in the course of booking the flight) and information on the legal basis for processing and the recipients of this data. The Complainant also requested the presentation of a list of data the Company holds about him. The Complainant did not receive a response to the request from the Company and expressed doubts as to the legality of requesting him to provide the additional data and their further processing by the Company. The Complainant demanded to oblige the Company to answer his inquiries.

In the course of the administrative proceedings, the President of the Personal Data Protection Office established the following facts.

1. On 22 August 2018, the Complainant travelled from Tallinn via Warsaw to Brussels on a flight operated by the Company.
2. At the airport in Warsaw, before boarding the plane, the Complainant was asked to provide additional information that had been collected on behalf of the authorities of the airport in Brussels. Additional information included the Complainant's data on: his citizenship, date of birth, number and expiry date of his identity card.
3. On 22 August 2018, the Complainant sent a request to the Company by an e-mail to the address [REDACTED], in which he called the Company to indicate: the legal basis for processing additional data (including data related to the travel document), despite the fact that these data they are not required in order for the Company to operate; why such information was required; whether the data has been or is to be transferred to any third party. The Complainant expressed doubts as to the legitimacy of obtaining by the Company his passenger data (API data) for intra-EU flights, although they are not required for the Company's operations. Moreover, the Complainant also demanded a catalogue of data that the Company holds about him (quoted as 'an overview of data that [REDACTED] has of me').
4. The company indicated that it did not receive the Complainant's request of 22 August 2018 for technical reasons, because (quotation): 'the e-mail box to which the e-mail was sent was subject to a closing procedure and such incidents could have occurred in exceptional cases'.
5. On 24 October 2018, the Complainant sent a message to the Company at [REDACTED], reminding the Company that he had not received a reply to his request of 22 August 2018, and asked to respond to its content.
6. The Company pointed out that the Complainant's second request (quotation) 'was not recognized due to the human factor – a former [REDACTED] associate accidentally marked the message received from the Complainant as "request resolved" and therefore it was not sent to the appropriate organizational unit of [REDACTED]'.

7. On 27 December 2018, the Complainant submitted a complaint to the Estonian supervisory authority. In the complaint, the Complainant indicated that he had not received a reply to his request for four months and that it was still not clear (and impossible to assess) why his data had been collected and whether the Company acted lawfully in collecting and processing his data. The Complainant also pointed out that the data of the travel document were not necessary in order for the Company to operate in the territory of the European Union and the Schengen area. The Complainant attached to the complaint a copy of the electronic correspondence, which he sent to the Company on 22 August 2018 and 24 October 2018. In the content of the complaint, the Complainant also indicated that he had received an automatic reply from the Company, in which the Company pointed out that his request was being examined and informed the Complainant that it was currently dealing with more requests than usual.
8. The complaint was transferred pursuant to Article 56 para. 1 of Regulation 2016/679 to the President of the Personal Data Protection Office, who took the case as the lead supervisory authority. The supervisory authorities that joined the proceeding as the supervisory authorities concerned are the Slovak, Dutch, French, Spanish, Danish, Norwegian and Italian supervisory authorities.
9. The Company in the explanations of 21 June 2019 indicated that this additional information was transferred to the authorities of the airport in Brussels pursuant to Article 3 para. 1 and 2 of Council Directive 2004/82/EC of 29 April 2004 and pursuant to the Belgian regulations implementing the above-mentioned directive, i.e. WEt van 15 mai 2006 betreffende diverse maatregelen inzake vervoer w związk z Arrêté royal du 18 juillet 2015 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers oraz Loi du 25 décembre 2016 relative au traitement des données des passagers. In the Company's opinion, the data was collected in accordance with Article 6 para. 1 of the directive mentioned above and were removed within 24 hours from the moment of their transfer and arrival of the means of transport, of which the Complainant was informed on 18 June 2019. The company also pointed out that 'after careful verification of the above-mentioned legal basis, [REDACTED] has ceased the practice of transferring personal data of passengers traveling with [REDACTED] and at present these data are not processed'.
10. The Company attached to the above-mentioned explanations a copy of the reply sent to the Complainant on 18 June 2019. In addition to the legal basis for the transfer of data to the Belgian authorities, the reply also indicated the current legal basis for the processing of his personal data, which, in the Company's opinion, is the legitimate interest of the data controller related to the performance of the contract of carriage of flights on the Tallinn (TLL) – Warsaw

(WAW) route on 21 August 2018 and on the Warsaw (WAW) – Brussels (BRU) route on 21 August 2018 for the purpose of storing them for archival (evidence) purposes or possibility of establishing and pursuing of claims or defending against potential claims arising from the performance of the contract of carriage until the claims under this contract are expired. In addition, the Company indicated what data in connection with the requirements of Article 3 para. 1-2 of Directive 2004/82/EC may be transferred to the authorities responsible for carrying out border checks at the external borders. The data includes the number and type of travel document used, nationality, full names, the date of birth, the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport and the initial point of embarkation. In reply, which was addressed to the Complainant, the Company did not indicate that it had ceased to provide the above-mentioned data of passengers traveling with [REDACTED]. The Company pointed out that the Complainant will obtain further information on the data processing processes on the website [REDACTED] in the tab ‘Regulation/Information about personal data processing’ ([REDACTED]).

11. On 26 June 2019, the Complainant forwarded, by e-mail, to the Personal Data Protection Office the correspondence between him and the Company conducted in the period of 18-25 June 2019. In that correspondence on 18 June 2019, the Complainant indicated that, in his opinion, the Company incorrectly identified the legal basis for the transfer of his personal data to Belgium, because the Directive 2004/82/EC allows carriers to transfer passenger data to state authorities in order to carry out checks at the external borders of the European Union (as specified in the first sentence of Article 6 para. 1 of the directive). Therefore, in the opinion of the Complainant, this directive cannot constitute a legal basis for the transfer of his personal data to Belgium, as it does not apply to intra-EU flights, i.e. flights made by the Complainant on the Tallinn-Warsaw-Brussels route. The Complainant also indicated the limited purpose of the processing permitted by the directive, which in Article 6 para. 1 is limited to data processing for the purposes of border control and the fight against illegal immigration. Moreover, the obligation to collect passenger data (API data) has been imposed on carriers for the sole purpose of combating illegal immigration from third countries, and carriers do not need this data for purposes related to their business activities. Moreover, the Complainant pointed out that the Company, referring to Belgian legal acts, also referred to Directive 2016/681, the so-called PNR Directive, since, as the Complainant identified himself, Belgian law refers to the act of 25 December 2016. The Complainant pointed out that the PNR Directive does not impose an obligation to collect API data for intra-EU flights. Their

collection is possible only when API data are part of PNR data indicated in Annex I of the PNR Directive and as indicated in Article 8 may only be collected insofar as carriers already collect this data in the course of their normal activities. The Complainant indicated that on intra-EU flights the collection of API data is not part of the carrier's normal operations. In connection with this, the Complainant pointed out that so far he had not obtained information on the legal basis for the processing of his personal data. Moreover, the Complainant requested confirmation of deletion of his personal data within 24 hours from the carriers' databases, in the event that the Company relies (although incorrectly) on the provisions of Directive 2004/82.

12. On 25 June 2019, the Complainant received a reply by e-mail from the Company, indicating that the Company had verified communications with the Member States regarding the transfer of API data and suspended the transfer of data to countries that are not entitled to receive them. Taking into account that the requirements imposed by Directive 2004/82/EC concern only the external borders of the European Union, the Company has suspended the transmission of API data to the Belgian authorities. The company indicated that the Complainant's personal data had been collected only at the request of the Belgian authorities and not for commercial purposes. The Company pointed out that Belgian law implementing the PNR Directive (Directive 2016/681) and the API Directive (2004/82/EC) indicates that air carriers for intra-EU flights departing from, to and through Belgium are obliged to provide API data and PNR if they already collect them in the normal course of their business. Due to the fact that the re-analysis of the Company confirmed that the request of the Belgian authorities exceeded the scope of the above-mentioned directive, the Company on 26 November 2018, suspended the provision of this data. The Company confirmed that the Complainant's API data has been deleted and is no longer processed by the Company.
13. In the message of 26 June 2019, redirecting the correspondence between the Complainant and the Company from the period of 18-25 June 2019 to the President of the Personal Data Protection Office and to the Estonian supervisory authority, the Complainant indicated that the Company finally admitted that it had collected excessive data about passengers, however, it only ceased to provide them to the Belgian authorities in November 2018, and that this data has been deleted.

After reviewing the entirety of the evidence collected in the case, the President of the Personal Data Protection Office considered the following.

Referring first of all to the legal basis for collecting and then transferring the Complainant's data, which were not obtained in the course of the Company's normal operations, to the Belgian

authorities, it should be stated that the Complainant's data were processed in this respect without any legal basis.

Pursuant to Article 3 para. 1 of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ EU L 261 of 06/08/2014, p. 24), hereinafter referred to as: the API Directive, it should be stated that the obligation of carriers to 'transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State', is limited to information on passengers traveling from third countries to the territory of one of the Member States. In connection with the above, indicated by the Company in response to the request of the President of the Personal Data Protection Office for explanations of 3 June 2019 and in the response addressed to the Complainant on 18 June 2019, the legal basis for the processing of the Complainant's personal data that were not obtained in the course of normal operations by the Company and their transfer to the Belgian authorities, in the form of Article 3 para. 1 and 2 of the API Directive and the provisions of Belgian law implementing it, was incorrectly indicated and could not, on 21 August 2018, constitute the legal basis for the transfer of the Complainant's data in the form of information on his citizenship, date of birth, number and expiry date of the identity card to the Belgian authorities (API data).

These data could be collected and transferred to the relevant Belgian authorities on the basis of Article 8 para. 1 of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name records (PNR) for the prevention, detection, investigation and prosecution of terrorist offenses and serious crime (OJ EU L 119 of 04/05/2016, p. 132), hereinafter referred to as: the PNR Directive, only to the extent that carriers already collected such data as part of their normal activities.

The established facts of the case show that the Company, in order to obtain these data from the Complainant, had to ask him to provide them before boarding. This means that the Company was not in possession of these data and did not obtain them in the course of its activities (e.g. in the course of booking airline tickets). The Company itself indicated in the explanations that (quotation): 'after careful verification of the above-mentioned legal basis, [REDACTED] has ceased the practice of transferring personal data of passengers traveling with [REDACTED] and at present this data is not being processed'. The Company also, in the reply addressed to the Complainant, indicated that on 26 November 2018, it suspended the disclosure of this data. The above analysis and the Company's behavior indicate that it did not have, at the time of obtaining and transmitting, the Complainant's API data, in the form of information such as about his travel document, the legal basis for processing.

It should be stated that the violation of Article 6 para. 1 of Regulation 2016/679 in this case lasted from 22 August 2018 to 23 August 2018, because on 23 August 2018, in accordance with Article 6 para. 1 of Directive 2004/82, within 24 hours from the arrival of the means of transport, the data was removed from the Company's database and from the databases of authorities responsible for border control, which delete the data, within 24 hours from the moment of transferring, unless the data is later needed to fulfill the statutory functions of the bodies responsible for carrying out checks on persons at the external borders (...). It should be noted, however, that from the facts of the case it follows that from at least 22 August 2018 to 26 November 2018, i.e. for at least 3 months, it collected and transferred the data of passengers traveling on intra-EU routes from, to and through the territory Belgium to the Belgian authorities without a legal basis.

However, the legal status was finally restored by the Company with the removal of the Complainant's API data from the Company's databases and with the cessation of collecting and transferring API data of other passengers of intra-EU flights offered by the Company to unauthorized authorities.

Referring to the date of the exercise of the right to access the Complainant's data, it should be noted that the original request of the Complainant was sent to the Company on 22 August 2018 to the e-mail address [REDACTED], then a reminder message was sent to the Company on 24 October 2018. The Complainant received a partial reply to his request only on 25 June 2019, because it was only in this message that the Company responded to his request regarding the legal basis for collecting and transferring his data in the form of, inter alia, information about his travel document and indicated that it did not have a legal basis for transmitting these data to the Belgian authorities. However, the Company has not yet complied with his request regarding the right to access the data, which he is entitled to pursuant to Article 15 para. 1 of Regulation 2016/679.

Pursuant to Article 12 para. 3 of Regulation 2016/679 '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, however, the Company should have informed the Complainant about such an extension within one month of receiving his request, stating the reasons for the delay. While the Company itself indicated that the first e-mail of the Complainant addressed to the e-mail address [REDACTED] on 22 August 2018 was never received by the Company, because 'the e-mail message to which the e-mail was sent , was subject to the closing procedure (...)', the Complainant in the content of the complaint indicated that he had received an automatic reply from the Company, in which the Company indicated that his

request was being examined and informed the Complainant that it was currently dealing with more requests than usual.

The e-mail of 24 October 2018 sent by the Complainant to the same e-mail address (████████) to which his original correspondence of 22 August 2018 was sent, was, as indicated by the Company, already received by it, but his request (quotation): ‘was not recognized due to the human factor – a former █████ associate accidentally marked the message received from the Complainant as ‘report terminated’ and therefore it was not sent to the appropriate organizational unit of █████’. The Company’s argumentation as justifying the delay in responding to the Complainant’s request should be considered incorrect, as the indicated problems resulting from the liquidation of the electronic mailbox or the behavior of one of its employees would not have occurred if the Company had trained its employees in such a way that they would be able to identify requests of data subjects and redirecting them to the relevant organizational units of the Company and if the Company implements technical measures that would enable the redirection of e-mail messages to inactive e-mail addresses in such a way that the data subjects could exercise their rights.

Moreover, it should be noted that no technical problem or human factor limits the Company’s liability for the untimely response to the Complainant’s request for access to his data. According to Article 12 para. 3 of Regulation 2016/679, the maximum deadline for the Company to respond to the Complainant’s request of 22 August 2018 was one month. The Company did not provide evidence that it informed the Complainant about the reasons for the delay and extended the deadline for replying by another two months within one month of receiving the Complainant’s request. Although the Company indicated that it never reached the Complainant’s request of 22 August 2018, it clearly indicated that it had received the Complainant’s message, sent to the same e-mail address, reminding of his case on 24 October 2018. This means that in the case of both messages (dated on 22 August 2018 and 24 October 2018), the Company exceeded the permissible time frame and would not have responded to the Complainant’s request, if the President of the Personal Data Protection Office did not intervene, calling the Company for explanations in a letter of 3 June 2019. The Company, despite the fact that it was obliged to respond within one month, did not comply with this obligation.

The assessment by the President of the Personal Data Protection Office serves in each case the legitimacy of sending an order to a specific subject corresponding to the instruction of Article 58 para. 2 letter d) of the Regulation 2016/679 to restore the lawful state in the process of data processing or the disposition of Article 58 para. 2 letter c) of the above-mentioned Regulation to meet the request of the data subject – these instructions are justified and necessary only insofar as irregularities in the processing of personal data still exist.

In this case, it was established that the collection and transmission of the Complainant's API data took place without a legal basis, while as regards continuation of processing, it should be noted that the Company restored the legal status by removing these data from its databases and by resigning from the transfer of passenger data to the Belgian authorities. However, the processing of API data of the Complainant in the period from 22 August 2018 to 23 August 2018 and the processing of API data of other passengers on intra-EU flights in the period from at least 22 August 2018 to 26 November 2018 is a violation of Article 6 para. 1 of the Regulation 2016/679, therefore the President of the Personal Data Protection Office issued a reprimand to the Company.

Referring to the Complainant's request for the Company to indicate the legal basis for the processing of additional data (including data related to the travel document), despite the fact that these data are not required for the purposes of the Company's business, the reasons for which such information was required, information if these data have been transferred or are to be transferred to any third party and to grant him access to the content of data that the Company has about him, violation of Article 12 para. 3 of Regulation 2016/679, to the extent to which the Complainant received only a partial response from the Company to the request in question, therefore the President of the Personal Data Protection Office issued a reprimand to the Company.

Referring to the failure to meet the Complainant's request to provide the list of data that the Company holds about him, it should be considered that so far the Company has not exercised in this respect his right to access the content of the data, to access which he is entitled to pursuant to Article 15 para. 1 of Regulation 2016/679. In response to the Complainant's request, the Company's response was limited to provide the address of the website [REDACTED]

[REDACTED]), where the Complainant can find information on data processing by the Company. The Company, therefore, failed to comply with the Complainant's request and did not grant him access to his data. Such activity of the Company is a violation of Article 15 para. 1 of the Regulation 2016/679, therefore the President of the Personal Data Protection Office, pursuant to Article 58 para. 2 letter c) of Regulation 2016/679 ordered the Company to grant the Complainant access to his personal data in the scope of the list of data that the Company has on him.

In this factual and legal background, the President of the Personal Data Protection Office adjudicated as in the operative part of this decision.

Under the authority of the President
of the Personal Data Protection Office

[REDACTED]

[REDACTED]

This decision is a final decision. Based on Article 7 para. 2 of the Act of 10 May 2018 on the protection of personal data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781 as amended) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2019, item 2325), the party has the right to bring a complaint to the Wojewódzki Sąd Administracyjny [Voivodship Court of Administration] in Warsaw against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Personal Data Protection Office, Stawki 2,00-193 Warsaw). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance, including exemption from court costs.

TRANSLATION

**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**
Jan Nowak

Warsaw, 6 July 2021

Ref. No.: ZSPR.440.1070.2018.PT.BS

(previous Ref. No.: ZSPR.440.1070.2018.LS.I)

DECISION

On the basis of Article 104 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735), Article 7 (1) of the Act of 10 May 2018 on personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781), Article 60 (8) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), regarding the complaint of [REDACTED]
[REDACTED], running a business under the name of [REDACTED]
[REDACTED] (address: [REDACTED]), on the irregularities in the processing of his personal data by [REDACTED]. based in Barcelona ([REDACTED]
[REDACTED]), consisting in the processing of personal data without a legal basis, President of the Personal Data Protection Office

rejects a complaint.

JUSTIFICATION

On 3 August 2018, the Personal Data Protection Office received a complaint from [REDACTED]
[REDACTED], running a business under the name of [REDACTED]
[REDACTED] (address: A [REDACTED]), hereinafter referred to as: the

Complainant, about irregularities in the processing of his personal data by [REDACTED] based in Barcelona ([REDACTED]), hereinafter referred to as: the Company, consisting in the processing of the complainant's personal data without a legal basis.

The President of the Personal Data Protection Office identified the case as having a cross-border nature in accordance with Article 4 (23) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), hereinafter referred to as: Regulation 2016/679, and referred the case to the Spanish supervisory authority (Spanish: *Agencia Española de Protección de Datos*), hereinafter referred to as: AEPD, which took the case as leading supervisory authority.

After conducting the proceedings on the submitted complaint, AEPD notified the President of the Personal Data Protection Office about the findings made by it and presented a proposal for resolving the matter by closing the case. The President of the Personal Data Protection Office agreed with the factual findings made by AEPD.

In the course of administrative proceedings, the President of the Personal Data Office Protection established the following facts:

1. On 18 June 2015, the Company concluded an agreement with [REDACTED].
The subject of the above-mentioned contract was to carry out the activity of collecting personal data of certain natural persons who showed interest in receiving advertising messages. The above contract specified the scope of personal data subject to the order: name, surname, gender, date of birth, e-mail address, time stamp or registration time and IP address. The contract also included the complementary service 'COI' (Opt-In confirmation), thanks to which [REDACTED] is obliged to apply the mechanism of double verification of the registration of the interested person in the database which is the subject of the contract, in order to guarantee the acquisition of data and the correct understanding and willingness to provide it by the user. The contract specifies the purpose of further data use by the Company – sending advertising messages using e-mail marketing techniques. In addition, it states that [REDACTED] V. is obliged to provide the interested party with information about the recipient of their data (which in this case was the Company), as well as about the methods of use / processing to

which the data will be subjected (in this case, for sending advertisements by electronic means) (AEPD findings of 9 February 2021).

2. The Complainant's personal data (including: name, surname, gender, date of birth, zip code, e-mail address, time stamp and IP address) were obtained by the Company on 7 March 2015 at 19:02 via the Internet promotional campaign organized by [REDACTED] [REDACTED], [REDACTED] run at the website: [REDACTED]. In the Company's opinion, the Complainant's consent to the processing of data for direct marketing purposes was deliberate because additional confirmation was necessary by clicking on the link in the e-mail received (AEPD findings of 9 February 2021).
3. The AEPD established that the Company had demonstrated that on 7 March 2015 the Complainant consented to the processing of his data in order to receive marketing e-mails (AEPD findings of 9 February 2021).
4. The findings of the AEPD show that the Company complied with the request and informed the Complainant about the deletion of his personal data, after receiving the Complainant's request to be removed from the Company's mailing list (AEPD findings of 9 February 2021).
5. The Complainant, via the 'Opt-Out' link in each marketing message sent directly or on behalf of the Company, on 22 June 2018 at 17:41, objected to the processing of his personal data for direct marketing purposes. The company stopped processing the Complainant's personal data (AEPD findings of 9 February 2021).

After reviewing the entirety of the evidence collected in the case, the President of the Office for Personal Data Protection considered the following.

It should be pointed out that Regulation 2016/679 defines the obligations of the data controller, which include the processing of personal data in compliance with the conditions set out in this regulation. The provision entitling data controllers to process ordinary data of natural persons, including their disclosure, is Article 6 (1) of Regulation 2016/679, according to which data processing is allowed only if one of the conditions indicated in this provision is met. The catalog of premises listed in Article 6 (1) of Regulation 2016/679 is closed. Each of the premises legalizing the processing of personal data is autonomous and independent. This means that these conditions are, in principle, equal, and therefore meeting at least one of them determines the lawful processing of personal data. As a consequence, the consent of the data subject is not the only basis for the processing of personal data, because the data processing process will be

compliant with Regulation 2016/679 also when the data controller demonstrates that another of the above-mentioned conditions is met. Regardless of the consent of the data subject (Article 6 (1) (a) of Regulation 2016/679), the processing of personal data is allowed, *inter alia*, when 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 (letter b); processing is necessary for compliance with a legal obligation to which the controller is subject (letter c); processing is necessary in order to protect the vital interests of the data subject or of another natural person (letter d); 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 (letter e); 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 (letter f).

At the outset, it should be noted that Article 21 of Regulation 2016/679 regulates the issue of the party's right to object to the processing of their personal data. In accordance with paragraph 2 and 3 above of the provision, if personal data are processed for direct marketing purposes, the data subject has the right to object at any time to the processing of his personal data for the purposes of such marketing, including profiling, to the extent that the processing is related to such marketing direct. If the data subject objects to processing for direct marketing purposes, the personal data may no longer be processed for such purposes.

Referring the above to the process of processing his personal data for marketing purposes questioned by the Complainant without a legal basis, it should be indicated that until the date of the Complainant's objection, i.e. until 22 June 2018, the Company processed his personal data on the basis of the consent expressed by the Complainant on 7 March 2015, and therefore this process was based on Article 6 (1) (a) of Regulation 2016/679, and during the period of the Act of 29 August 1997 on the protection of personal data (Dz. U. [Journal of Laws] of 2016, item 922, as amended), it was legal pursuant to Article 23 (1) (1) of this act.

As follows from the evidence collected in this case, the questioned sending of the information containing the marketing offer took place after the Complainant consented to the processing of his personal data for marketing purposes on 7 March 2015, but before he submitted an objection on 22 June 2018. The above means that the Company did not breach the provisions on the protection of personal data, as this process was based on Article 6 (1) (a) of Regulation 2016/679.

It should be noted here that the administrative procedure conducted by the President of the Personal Data Protection Office serves to control the compliance of data processing with the provisions on the protection of personal data and is aimed at issuing an administrative decision restoring the legal status pursuant to Article 58 (2) of Regulation 2016/679. The assessment made by the President of the Personal Data Protection Office in each case serves to examine the legitimacy of issuing an order to a specific subject corresponding to the disposition of Article 58 (2) of Regulation 2016/679 to restore the lawful state in the data processing process – so it is justified and necessary only insofar as there are irregularities in the processing of personal data. In the opinion of the President of the Personal Data Protection Office, there are no grounds to conclude that such irregularities exist in this case, because the processing of Complainant's personal data by the Company for marketing purposes questioned by him, was based on Article 6 (1) (a) of Regulation 2016/679.

In this factual and legal background, the President of the Personal Data Protection Office adjudicated as in the sentence.

Under the authority of the President
of the Personal Data Protection Office



This decision is a final decision. Based on Article 7 (2) of the Act of 10 May 2018 on the Protection of Personal Data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2019, item 2325), the party has the right to bring a complaint to the Provincial Administrative Court in Warsaw against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00 – 193 Warszawa [Personal Data Protection Office, Stawki 2, 00-193 Warsaw]). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of assistance may be granted upon application by a party submitted prior to the initiation of the proceedings or in the course of the proceedings. This application is free of court fees.

TRANSLATION

**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**

Jan Nowak

Warsaw, 8 July 2021

Ref. No.: DS.523.839.2021.PT.BS

DECISION

On the basis of Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735) and Article 7 para. 1 of the Act of 10 May 2018 on the personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781) in the case of [REDACTED], residing in [REDACTED] at [REDACTED] [REDACTED], relating to irregularities in the processing of his personal data by [REDACTED] [REDACTED] with its headquarters in Malta (address: [REDACTED] [REDACTED]), consisting in disclosing personal data of [REDACTED] by [REDACTED] [REDACTED]. for [REDACTED] with its headquarters in Wrocław (address: [REDACTED] [REDACTED]), without legal basis, the President of the Personal Data Protection Office

decides to discontinue the proceedings.

JUSTIFICATION

On 7 May 2019, the Personal Data Protection Office received a complaint from [REDACTED] [REDACTED], residing in [REDACTED] at [REDACTED] hereinafter referred to as the Complainant, on irregularities in the processing of his personal data by [REDACTED] with its headquarters in Malta (address: [REDACTED] [REDACTED]), consisting in disclosing the Complainant's personal data by [REDACTED] for [REDACTED] with its headquarters in Wrocław (address: [REDACTED] [REDACTED]), without legal basis.

On 6 July 2021, the Personal Data Protection Office received a letter from the Complainant informing that he withdraws the complaint submitted to the President of the Personal Data Protection Office.

Due to the withdrawal of the complaint, the proceedings became redundant, and the present proceedings are subject to discontinuation pursuant to Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735), hereinafter referred to as the Code of Administrative Procedure. In accordance with the above-mentioned provision, when the proceedings for any reason have become redundant in whole or in part, the public administration authority shall issue a decision to discontinue the proceedings, respectively, in whole or in part. The wording of the above-mentioned regulation leaves no doubt that in the event that the proceedings are deemed groundless, the authority conducting the proceedings will obligatorily discontinue them.

The determination by the public authority of the existence of the premise referred to in Article 105 § 1 of the Code of Administrative Procedure obliges it, as it is emphasized in the doctrine and jurisprudence, to discontinue the proceedings.

In this factual and legal background, the President of the Personal Data Protection Office adjudicated as in the sentence.

Under the authority of the President
of the Personal Data Protection Office



This decision is a final decision. Based on Article 7 para. 2 of the Act of 10 May 2018 on the Protection of Personal Data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2019, item 2325), the party has the right to bring a complaint to the Provincial Administrative Court in Warsaw against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Personal Data Protection Office, Stawki 2, 00-193 Warsaw). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of assistance may be granted upon application by a party submitted prior to the initiation of the proceedings or in the course of the proceedings. This application is free of court fees.

TRANSLATION

**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**

Jan Nowak

Warsaw, 10 November 2021

ZSPR.440.1779.2019.PT.WU

Previous Ref. No.: **ZSPR.440.1662.2019.ZS.MKA**

DECISION

On the basis of Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735), and Article 7 paragraph 1 and 2 of the Act of 10 May 2018 on the personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781) and Article 60 (8) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35) after having carried administrative proceedings in the case of [REDACTED], residing in [REDACTED]
[REDACTED], relating to irregularities in the processing of his personal data by [REDACTED]
[REDACTED] based in Budapest, [REDACTED], by failing to comply with the request to erase his personal data, the President of the Personal Data Protection Office

shall discontinue the proceedings.

Justification

The Personal Data Protection Office received a complaint from [REDACTED], residing in [REDACTED], hereinafter referred to as the Complainant, on irregularities in the processing of his personal data by [REDACTED] with its registered office in Budapest [REDACTED], hereinafter referred to as the Company, consisting in failure to comply with the request to erase his personal data.

In the course of the administrative proceedings, the President of the Personal Data Protection Office, hereinafter also referred to as the President of the Office, established the following facts.

1. The Complainant received unwanted marketing messages at his email addresses: [REDACTED], [REDACTED], [REDACTED] and [REDACTED];
2. The Complainant used the "wypisz się/unsubscribe" button in order not to receive further messages;
3. The Complainant also requested by an email to discontinue sending marketing messages to his email addresses;
4. Regarding the cross-border nature of proceedings pursuant to Article 4(23) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119 of 04/05/2016, p. 1, OJ EU L 127 of 23/05/2018, p. 2 and OJ EU L 74 of 04/03/2021, p. 35), hereinafter referred to as: GDPR, pursuant to Article 56(1) GDPR the proceedings has been referred to the lead supervisory authority, which is the Hungarian supervisory authority (Nemzeti Adatvédelmi és Információszabadság Hatóság), hereinafter referred to as the 'Hungarian Supervisory Authority';
5. The Hungarian Supervisory Authority considered itself to be the lead authority on 16 January 2020 based on the fact that the Company has its headquarters in Hungary;
6. The Hungarian Supervisory Authority asked the President of the Office to provide documents certifying that there is a button or a link in the emails sent by the Controller to unsubscribe from the newsletter;
7. On 9 June 2020, the President of the Office asked the Complainant to provide documents confirming that in the emails sent by the Controller there is a button or a link to unsubscribe from receiving the newsletter;
8. The Complainant attached to the letter of 9 June 2020 his e-mail correspondence with the Company confirming that in the emails sent by the Company there is a link to unsubscribe from receiving the newsletter;
9. The President of the Office forwarded to the Hungarian Supervisory Authority the documents which received from the Complainant together with their translation into English;

10. The Hungarian Supervisory Authority informed that it had contacted the Company, which informed that it was not the owner of the domains from which marketing messages are sent to the Complainant;
11. The Hungarian Supervisory Authority issued a draft decision in the case in which it concluded that in relation to the finding that it is not the Company that is sending marketing messages to the Complainant, it is not the lead authority within the meaning of Article 56(1) GDPR and ended the proceedings;
12. The President of the Office did not raise a reasoned objection to the draft decision and agreed with the draft decision prepared by the Hungarian Supervisory Authority;
13. In relation to the dismissal of the Complainant's complaint by the Hungarian Supervisory Authority, the President of the Office, pursuant to Article 60(8) GDPR, as the authority receiving a complaint, is obliged to adopt a decision.

The President of the Office, after reviewing all the evidence gathered, considered the following.

The Complainant indicated in the complaint that the company [REDACTED] [REDACTED] with its registered office in Budapest, at [REDACTED], as a defendant. The President of the Office, acting as a public authority, is bound by the content of the complaint and the scope of the party's request.

It should be pointed out that the President of the Office, when issuing an administrative decision, is obliged to decide on the basis of the facts existing at the time of the adoption of that decision. As stated in the legal doctrine, "the public authority shall assess the facts of the case at the time when the administrative decision was adopted. This rule also applies to the assessment of the legal status of the case, which means that the public authority issues an administrative decision on the basis of the legal provisions in force at the time of its adoption (...). Adjudication in administrative proceedings consists of applying the law to the established facts of an administrative case. In this way the public authority pursues the purpose of administrative proceedings, which is to implement a binding legal norm in administrative-legal relations, when these relations require it" (Commentary to the statute of 14 June 1960, Code of Administrative Procedure, M. Jaśkowska, A. Wróbel, Lex., el/2012). Furthermore, in the judgment of 7 May 2008 in the case Ref. No. I OSK 761/07, the Polish Supreme Administrative Court stated that "when examining the lawfulness of personal data processing, the GODO is obliged to determine whether, on the date of issuing a decision in the case, data of a particular entity are processed and whether this is done in a lawful manner".

The decisive factor for the decision to be issued in this case is the fact that the Company does not process the Complainant's personal data and is not the Controller of the domains from which the Complainant receives unwanted marketing messages.

Under these circumstances, the present proceedings are subject to discontinuation pursuant to Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735), hereinafter referred to as Kpa, due to the fact they have become devoid of purpose. Under that provision, where the proceedings have for any reason become devoid of purpose in whole or in part, the public authority is to issue a decision to discontinue the proceedings in whole or in part, respectively. The wording of that provision leaves no doubt that, if the proceedings is found to be devoid of purpose, the authority conducting the proceedings mandatorily discontinues them. At the same time, the literature on the subject-matter indicates that the administrative procedure devoid of purpose, as provided for in Article 105(1) of the Code of Administrative Procedure, means that there is no element of a substantive legal relationship and, therefore, no decision can be taken to settle the case by deciding on the merits of the case (B. Adamiak, J. Borkowski 'Code of Administrative Procedure. Commentary' 7th edition, C.H. Beck, Warsaw 2005, p. 485). The same position was taken by the Provincial Administrative Court in Cracow in its judgment of 27 February 2008 (III SA/Kr 762/2007): "Proceedings shall become devoid of purpose if one of the elements of the substantive relationship is absent, which means that the case cannot be settled by a decision on the merits".

The assessment carried out by the President of the Office shall in each case examine the validity of referring to a particular entity a decision corresponding to the content of Article 58(2) GDPR, which is intended to restore the lawful state of the processing of data - is therefore justified and necessary only insofar as the processing of personal data in question exists.

In this factual and legal state, the President of the Personal Data Protection Office adjudicated as in the operative part.

Under the authority of the President
of the Personal Data Protection Office



This decision is a final decision. Based on Article 7 para. 2 of the Act of 10 May 2018 on the Protection of Personal Data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2019, item 2325), the party has the right to bring a complaint to the Wojewódzki Sąd Administracyjny w Warszawie [Voivodeship Administrative Court in Warsaw] against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Urząd Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of assistance may be granted upon application by a party submitted prior to the initiation of the proceedings or in the course of the proceedings. This application is exempt from court fees.

TRANSLATION

PRESIDENT OF THE PERSONAL DATA PROTECTION OFFICE

Jan Nowak

Warsaw, 24 March 2022

Ref. No.: DS.523.2928.2021.ZS.BS

DECISION

On the basis of Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735 as amended) and Article 7 para. 1 of the Act of 10 May 2018 on the personal data protection (consolidated text: Dz. U. [Journal of Laws] of 2019 item 1781) in the case of Ms. ██████████, residing in ██████████, relating to irregularities in the processing of her personal data by ██████████ with its headquarters in Luxembourg (address: ██████████, Luxembourg), consisting in a request to send a copy of an ID card, failure to comply with the request to erase data, failure to comply with the information obligation and failure to comply with the request to access personal data of Ms. ██████████, the President of the Personal Data Protection Office

decides to discontinue the proceedings.

JUSTIFICATION

The Personal Data Protection Office received a complaint from Ms. ██████████, residing in ██████████, hereinafter referred to as the Complainant, relating to irregularities in the processing of her personal data by ██████████ with its headquarters in Luxembourg (address: ██████████, Luxembourg), consisting in a request to send a copy of an ID card, failure to comply with the request to erase data, failure to comply with the information obligation and failure to comply with the request to access personal data of the Complainant.

On 24 February 2022, the Personal Data Protection Office received a letter from the Complainant informing that she withdraws the complaint lodged with the President of the Personal Data Protection Office.

Due to the withdrawal of the complaint, the proceedings became redundant, and these proceedings are subject to discontinuation pursuant to Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Dz. U. [Journal of Laws] of 2021 item 735

as amended), hereinafter referred to as the Code of Administrative Procedure. In accordance with the above-mentioned provision, when the proceedings for any reason have become redundant in whole or in part, the public administration authority shall issue a decision to discontinue the proceedings, respectively, in whole or in part. The wording of the above-mentioned regulation leaves no doubt that in the event that the proceedings are deemed groundless, the authority conducting the proceedings will obligatorily discontinue them.

The determination by the public authority of the existence of the premise referred to in Article 105 § 1 of the Code of Administrative Procedure obliges it, as it is emphasized in the doctrine and jurisprudence, to discontinue the proceedings.

In this factual and legal background, the President of the Personal Data Protection Office adjudicated as in the sentence.

Under the authority of the President
of the Personal Data Protection Office
Director of the Complaints Department
[REDACTED]

This decision is a final decision. Based on Article 7 para. 2 of the Act of 10 May 2018 on the protection of personal data (consolidated text: Dz. U. [Journal of Laws] of 2019, item 1781) and in connection with Article 13 § 2, Article 53 § 1 and Article 54 of the Act of 30 August 2002 Law on proceedings before administrative courts (consolidated text: Dz. U. [Journal of Laws] of 2022, item 329), the party has the right to bring a complaint to the Wojewódzki Sąd Administracyjny w Warszawie [Provincial Administrative Court in Warsaw] against this decision, within 30 days from the date of delivery of this decision, through the President of the Personal Data Protection Office (address: Personal Data Protection Office, Stawki 2, 00-193 Warsaw). The fee for the complaint is PLN 200. The party has the right to apply for the right of assistance.



**PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**
Jan Nowak

Warsaw, 29 July 2022

DS.523.2402.2020.ZS.JKO.

DECISION

Pursuant to Article 104 § 1 and Article 105 § 1 of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws 2021, item 735, as amended) in connection with Article 7(1) of the Act on Personal Data Protection of 10 May 2018 (Journal of Laws of 2019, item 1781), Article 5(1)(a), Article 5(2), Article 12 (1), Article 13(1)(a), (c) and (e), Article 13(2)(a)(b)(d) and (e) and Article 58(2)(c) of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Journal of Laws EU L 119 of 04.05.2016, p. 1 and Journal of Laws of the EU L 127 of 23.05.2018, p. 2 and Journal of Laws UE L 74 of 4.03.2021, p. 35) (hereinafter: GDPR), having conducted an administrative proceedings concerning the complaint lodged by [REDACTED] (address: [REDACTED]
[REDACTED], Lithuania), regarding the irregularities in the processing of his personal data by [REDACTED] and [REDACTED], who conduct business activity under the name [REDACTED],
[REDACTED] (address: [REDACTED] Poland), (hereinafter: collectively referred to as Entrepreneurs), consisting in sharing personal data with third parties, failing to comply with the obligation to provide information and failing to provide access to data, the President of the Personal Data Protection Office

- 1. orders [REDACTED] and [REDACTED], pursuing business activity as part of the civil partnership under the name [REDACTED]
[REDACTED] (address: [REDACTED]
[REDACTED] Poland), to comply with the obligation of [REDACTED], residing at [REDACTED] Lithuania, the information obligation pursuant to Article 13 (1) (a), (c), (e) and para. (2) (a), (b), (d),(e) of the Regulation (EU)**

2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Journal of Laws EU L 119 of 04.05.2016, p. 1 and Journal of Laws of the EU L 127 of 23.05.2018, p. 2 and Journal of Laws UE L 74 of 4.03.2021, p. 35), by sending the required information to the Complainant's correspondence address or email address,

- 2. in the remaining scope it discontinues the proceedings.**

Justification

The Personal Data Protection Office has received from the Lithuanian Supervisory Authority (hereinafter: Lithuanian SA), through the Internal Market Information System between supervisory authorities (IMI system), a complaint case regarding irregularities in the processing of personal data of [REDACTED] (residing at [REDACTED]
[REDACTED], Lithuania), hereinafter referred to as: "the Complainant", by [REDACTED]
and [REDACTED], conducting business under the name [REDACTED]
[REDACTED], [REDACTED] (address: [REDACTED], Poland), hereinafter collectively referred to as the "Entrepreneurs", in connection with the sharing of the Complainant's personal data with third parties, failure to comply with the information obligation and failure to grant the Complainant access to the data. The Polish Supervisory Authority, namely the President of the Personal Data Protection Office (hereinafter: "President of the PDPO"), having analysed the facts of the case, considered itself in the present case to be the lead supervisory authority (LSA) pursuant to Article 56(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (Journal of Laws EU L 119 of 04.05.2016, p. 1 and Journal of Laws of the EU L 127 of 23.05.2018, p. 2 and Journal of Laws UE L 74 of 4.03.2021, p. 35) - hereinafter referred to as: "GDPR", due to the registered office of the Entrepreneurs, which was located on the territory of Poland, as informed by the Lithuanian SA during the proceedings.

In the content of the complaint dated on 18 November 2019, transmitted in the IMI system by the Lithuanian SA on 26 February 2020, the Complainant indicated that the Entrepreneurs violated its rights, did not comply with the sales regulations, European guarantee obligations and rules on personal data protection. Complainant also indicated,

that the Entrepreneurs shared his personal data with third parties. The Complainant further pointed out that the rules for processing personal data were not available on the Entrepreneurs' website, he was not provided with information about the data processing, and he was not granted the right of access to the data.

In the course of the proceedings conducted in the present case, the President of the PDPO as the LSA, established the following factual state.

1. On 10 June 2020, the President of the PDPO, through the Lithuanian SA, informed the Complainant that this complaint case has been identified as cross-border nature pursuant to Article 4(23) of the GDPR and has been forwarded to the Polish SA for conduct;
2. On 10 June 2020, the President of the PDPO requested the Entrepreneurs to respond to the content of the complaint and to provide explanations in the case;
3. In explanations received by the Personal Data Protection Office on 26 June 2020, the Entrepreneurs indicated the following:
 - a. On 10 July 2019, Entrepreneurs concluded a contract with Complainant for the sale of the "Dorado" kayak [online store: ██████████ /];
 - b. the Complainant's personal data are processed on the basis of Article 6(1)(b) GDPR, which means that the processing was necessary for the performance of a contract to which the Complainant was a party;
 - c. Entrepreneurs indicated that the scope of data processed includes the name and surname, address, telephone number and e-mail address;
 - d. the Complainant's personal data were not shared with third parties; the Entrepreneurs pointed out that the content of the complaint does not indicate when, and most importantly to which entities, the data were to be shared;
 - e. The information obligation is fulfilled for customers of the online store who decide to make a purchase via the website ██████████. Customers must accept the store's regulations (Terms and Conditions of Service), which specify in detail for what purpose customer data are processed and what rights are granted in this connection. The Regulations are available on the Entrepreneurs' website, and the Complainant decided to purchase a kayak by sending an inquiry in the form of an e-mail to the address ██████████ also appearing on the aforementioned website;

- f. The Complainant never approached the Entrepreneurs with a request for access to the processed data. The Complainant has not submitted any evidence to prove this, despite making an allegation of this content against the Entrepreneurs.
4. On 17 July 2020, the Polish SA i.e. the President of the PDPO, provided the Complainant with as part of informal consultations through the Lithuanian SA, the Entrepreneurs' explanations translated in English;
 5. On 20 July 2020, the Polish SA i.e. the President of the PDPO, submitted to the Complainant, through the Lithuanian SA, a request for explanations in order to supplement the evidence collected in the case. The scope of explanations included the following questions:
 - a. when and to which entity Entrepreneurs shared the Complainant's personal data
 - b. when, in what form and to what extent the Complainant approached the Entrepreneurs with a request for access to data. Please provide the content of the request and confirmation that it was addressed to the Entrepreneurs.
 6. The Complainant did not respond to a request for an explanations dated 20 July 2020;
 7. On 24 July 2020, the Polish SA i.e. the President of the PDPO informed the Entrepreneurs about the above and at the same time asked for supplementation of the explanations submitted in the case;
 8. On 17 August 2020, the President of the PDPO received the Entrepreneurs' response to the above dated 11 August 2020, in which it was indicated that the Entrepreneurs implement the information obligations to the extent and in the manner indicated in the previous letter [i.e. dated June 2020]. Additionally, it was indicated that the Entrepreneurs have used the services of an entity offering professional and complex services in the area of implementation and proper performance of all obligations under GDPR, which means that in the near future, any irregularities, if identified, will be removed by the Entrepreneurs;
 9. On 13 October 2020, the Polish SA i.e. the President of the PDPO, provided the Complainant through the Lithuanian SA, additional explanations of the Entrepreneurs translated to English;
 10. On 13 October 2020 the Polish SA sent to the Lithuanian SA an e-mail with a request for information whether the Complainant received a request for explanations in order to supplement the evidence gathered in the case, which was forwarded through the IMI system by the Polish SA on 20 July 2020 (reply of the Lithuanian SA about forwarding the letter on 30 July 2020) and whether the Complainant responded to the letter;

11. On 20 October 2020, the Lithuanian SA responded via email indicating, that the Complainant had received the letter, but had not responded. Additionally, on 15 October 2020, the Lithuanian SA contacted the Complainant and determined, that the Complainant did not intend to respond to the received letter.

On these facts, the President of the PDPO has considered the following.

Indicate that, the President of the PDPO, when issuing an administrative decision, is obliged to adjudicate based on the factual state at the time of the decision. As indicated in the doctrine, “the public administration body assesses the factual state of the case according to the moment of issuing the administrative decision. This rule also applies to the assessment of the legal state of the case, which means that the public administration authority issues an administrative decision on the basis of the provisions of law in force at the time of its issuance (...). Adjudication in administrative procedures consists in applying the law in force to the established factual state of an administrative case. In this way, the public administration body realizes the purpose of administrative procedures, which is the implementation of the binding legal norm in the field of administrative-legal relations, when such relations require it” (Commentary to the Act of 14 June 1960 Code of Administrative Procedure M. Jaśkowska, A. Wróbel, Lex., el/2012). Furthermore, in the judgment of 7 May 2008 in the case with reference number I OSK 761/07 The Supreme Administrative Court stated that “when examining the legality of the processing of personal data, GIODO¹ is obliged to determine whether the data of a specific entity are processed on the date of adjudicating the case and whether it is conducted in accordance with the law”.

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"). The principle of transparency is further detailed in Article 12(1) of the GDPR, according to which 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.

Transparency is an overriding obligation under the GDPR that applies, among other things, to the provision of information to data subjects. “The principle of transparency requires

¹currently the President of the Personal Data Protection Office.

that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed" (Recital 39 GDPR). Therefore, it is important that the information addressed to the data subject is concise, clear, understandable and easily accessible, and in clear and plain language.

With regard to the Complainant's request for an order requiring the Entrepreneurs to comply with the obligation to provide information pursuant to Article 13(1) and (2) of the GDPR, it must be pointed out that this obligation should be complied by the controller at the time of obtaining the data, if the personal data were obtained from the data subject. The controller shall then be obliged to provide the following information: his identity and contact details and, where applicable, those of his representative (Article 13(1)(a)), where applicable - the contact details of the Data Protection Officer (Article 13(1)(b)), the purposes of the processing of personal data, and the legal basis for the processing (Article 13(1)(c)), where the processing is based on Article 6(1)(f) - the lawful interests pursued by the controller or by a third party (Article 13(1)(d)), information on the recipients of the personal data or categories of recipients, if any (Article 13(1)(e)), where applicable - information on the intention to transfer personal data to a third country or an international organisation and on whether or not the Commission has made a finding of adequate protection or, in the case of transfers referred to in Article 46, Article 47 or the second subparagraph of Article 49(1), information on adequate or appropriate safeguards, and the possibility of obtaining a copy of the data or of making the data available (Article 13(1)(f)).

Additionally, in accordance with Article 13(2) of the GDPR., in addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period (Article 13 (2)(a)); the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability (Article 13(2)(b)); where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal (Article 13(2)(c)); the right

to lodge a complaint with a supervisory authority (Article 13(2)(d); whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data (Article 13(2)(e)); 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 (Article 13(2)(f)).

As established in the course of the investigation, the Entrepreneurs were obliged - at the time of obtaining the Complainant's personal data - to provide the Complainant information specified in Article 13 in terms of paragraphs (1)(a),(c),(e) and (2)(a),(b),(d),(e) of the GDPR. In the present case, Article 13 (1)(b)(d)(f) and (2)(c) and (f) are not applicable. The Entrepreneurs conduct their business through the website [REDACTED] offering to purchase kayaking equipment online, based on an already existing kayak store that manufactures kayaks, belaying vests and life jackets i.e. [REDACTED]. Entrepreneurs also offer specialized kayak clothing and various accessories. The Entrepreneurs' Privacy and Data Processing Policy, hereinafter referred to as the "Privacy Policy", is available under the "Terms and Conditions" in §6 "Personal Data Security Policy" on the Entrepreneurs' website i.e. [REDACTED]. The Privacy Policy, which is available on the Entrepreneurs' website, is therefore not presented in an easily accessible and transparent form for the Complainant. The Privacy Policy, in order to satisfy the requirements of transparency and easily accessible form, should be located in a separate section and contain all necessary information concerning the processing of personal data by Entrepreneurs. In particular, it should be emphasized that the Entrepreneurs offer the purchase of equipment to customers outside the territory of Poland, such as the Complainant, and on the indicated website the Regulations of the online store are available only in Polish, so taking appropriate measures also refers to the understandable form of the Privacy Policy, which should be adapted in this case to international customers. In the course of the proceedings it was also established that the Entrepreneurs concluded the agreement for purchase of a kayak with the Complainant in a non-standard way, i.e. via e-mail. The Entrepreneurs did not substantiate that they fulfilled the information obligation at the moment of obtaining the Complainant's personal data, therefore the President of the PDPO, on the basis of the evidence gathered and all circumstances of the case, decided that the information obligation towards the Complainant was not fulfilled. The information obligation on Entrepreneurs is fulfilled only if it is provided in a simple, understandable and easily accessible

form. Placing the information obligation as part of the Regulations does not comply with the principle of transparency.

It is important to note that, the Privacy Policy is a document containing information that determines the correct fulfilment by Entrepreneurs of the obligation arising from Article 13 of the GDPR. The Privacy Policy should therefore contain information related to the processing of data of the data subject, otherwise the document does not comply with the condition of transparency and it is necessary to extract information and match it with the data processing, in which the data subject is involved.

Therefore, it is difficult to agree with the position of the Entrepreneurs that „the Company fulfils its information obligations towards the store's customers who, when deciding to purchase the Company's products via [REDACTED] must accept the store's regulations (Terms of Service), in which it is specified in detail for what purpose the customers' data are processed and what rights they have in this connection. These regulations are published on the Company's website, and the Complainant decided to purchase a kayak by sending an e-mail to [REDACTED]”. The Regulations, as stated above, are not a Privacy Policy. The regulations should contain information on e.g. terms of sale, methods of payment and delivery of goods or the possibility of withdrawal from the contract by the consumer. As the Article 29 Working Party pointed out in its "Guidelines on Transparency under Regulation 2016/679², privacy notices should be individually designed - a generic notice of the privacy policy of the owning or distributing company (...) is insufficient. It was the Entrepreneurs' obligation to provide information to the Complainant who made a non-standard purchase via email. The information placed in the Terms and Conditions (Regulations) on the Entrepreneurs' website does not satisfy the information obligation under Article 13(1) and (2) of the GDPR in this case. The Privacy Policy shall contain all information pursuant to Article 13 of the GDPR and comply with the requirements of Article 12(1) of the GDPR, in a clear and precise language form, understandable to all users, including the Complainant.

For the above reasons, it should be stated that not only the content, but also the form and the way in which the information should be provided to the data subject are important. Therefore, the solution applied by the Entrepreneurs in the form of placing the Privacy Policy in the Terms and Conditions does not comply with the requirements set out in Article 5(1)(a) and 12(1) of the GDPR.

²Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936.

In connection with the above, it should be pointed out that the Entrepreneurs violated Article 13(1)(a),(c),(e) and (2)(a),(b),(d),(e) of the GDPR, as they did not provide the Complainant with the indicated information when obtaining his personal data.

Pursuant to Article 58(2)(c) of the GDPR, each supervisory authority shall have of the following investigative powers, the power to order the controller or processor to comply the data subject's requests to exercise his or her rights pursuant to this Regulation. In view of the above, the President of the PDPO considers it reasonable to order the Entrepreneurs to comply with the information obligation towards the Complainant with regard to the identified violation of the provisions of Article 13(1)(a)(c)(e) and (2)(a)(b)(d)(e) of Regulation (EU) 2016/679 in the form of the information obligation.

At the same time it should be stated that, the remaining irregularities in the processing of the Complainant's personal data raised in the complaint are unfounded. The public administration authority may consider the facts of the resolved case as established only on the basis of undisputed evidence and may not rest on probability in this regard - unless the provisions of the Act of 14 June 1960 Code of Administrative Procedure (Journal of Laws 2021, item 735, as amended), hereinafter referred to as "kpa", provide differently. As stated by the Supreme Administrative Court in the judgment of 9 July 1999 (III SA 5417/98) "the authority conducting proceedings must strive to establish the material truth and according to its knowledge, experience and internal conviction assess the probative value of particular means of evidence, the impact of proof of one circumstance on other circumstances". In the same judgment the Court also stated that in administrative proceedings the principle applies that the burden of proof rests with the party who derives legal consequences from a given fact.

The Complainant correctly received a request for explanation from the Polish SA on 20 July 2020 through the Lithuanian SA, but did not provide any response to it. The scope of the Complainant's explanations was necessary to supplement the evidence and included establishing when and for which entity the Entrepreneurs provided access to the Complainant's personal data, and when, in what form and to what extent the Complainant addressed the Entrepreneurs with a request for access to the data. The Complainant was also informed in the summons, that failure to respond to the explanations may result in failure to prove the claims and allegations presented by the Complainant and, consequently, in the examination of the facts of the case and making a decision on the basis of the evidence gathered so far. Additionally, on 15 October 2020, the Lithuanian SA contacted the Complainant and established that it did not intend to respond to the letter received. It follows from the above that the Complainant did not want to participate in the proceedings or submit relevant explanations

and evidence in the case. Therefore, in the opinion of the President of the PDPO in the absence of sufficient evidence to prove the irregularities raised in the complaint, the President of the PDPO is not in a position to continue the proceedings and decide on the merits of the case.

In this situation, these proceedings are discontinued pursuant to Article 105 § 1 of the Act of 14 June 1960, Code of Administrative Procedure (hereinafter: "k.p.a."), because it is devoid of purpose. Pursuant to the aforementioned provision, if the proceedings have become, for whatever reason, wholly or partially pointless, the public administration authority shall issue a decision to discontinue the proceedings in whole or in part, respectively. The meaning of the above regulation leaves no doubt that in the event of determining that the proceedings have no purpose, the authority conducting these proceedings shall obligatorily discontinue them. At the same time, the literature on the subject indicates that the aimlessness of administrative proceedings, as provided for in Article 105 § 1 of the Code of Administrative Procedure means that any of the elements of a substantive legal relationship is absent, and therefore it is not possible to issue a decision that settles the matter by deciding it on the merits (B. Adamiak, J. Borkowski "Code of Administrative Procedure. Commentary" 7th edition, publishing house C.H. Beck, Warsaw 2005, p. 485). The same position was taken by the Provincial Administrative Court in Krakow in the judgment of 27 February 2008. (III SA/Kr 762/2007): "A proceeding becomes pointless when any of the elements of the substantive legal relationship is absent, which means that the case cannot be settled by a decision on the merits."

Establishment by the public authority of the existence of the prerequisite referred to in Article 105 § 1 of the Code of Administrative Procedure obliges it to discontinue the proceedings, because then there are no grounds for resolving the case as to its merits, and continuation of the proceedings in such a case would constitute its defect having a significant impact on the outcome of the case.

In this factual and legal state, the President of the PDPO has adjudicated as indicated in the operative part of the decision.

**Under the authority of the President
of the Personal Data Protection Office
Director of the Complaints Department**



The decision is final. Pursuant to Article 7(2) of the Act of 10 May 2018 on the Protection of Personal Data (Journal of Laws 2019, item 1781) in connection with Article 13 § 2, Article 53 § 1 and Article 54 § 1 of the Act of 30 August 30 2002 Law on Procedure before Administrative Courts (Journal of Laws 2022, item 329, as amended), the party has the right to lodge a complaint against this decision with the Voivodeship Administrative Court in Warsaw, within 30 days from the date of its delivery to the party. The complaint is lodged via the President of the Personal Data Protection Office. The fee for the complaint is in the amount of 200 PLN. The party has the right to apply for the right of aid, which includes exemption from court costs and the appointment of an attorney, legal advisor, tax advisor or patent attorney. The right of aid may be granted upon the request of a party submitted before the initiation of the procedure or in the course of the procedure. This request is free of court fees.



**THE PRESIDENT
OF THE PERSONAL DATA
PROTECTION OFFICE**

Jan Nowak

Warsaw, 24.11.2022

DS.523.1676.2021.ZS.WU

DECISION

Pursuant to Article 105(1) of the Act of 14 June 1960 Code of Administrative Procedure (consolidated text: Journal of Laws Of Laws 2022, item 2000), Article 7(1) and 7(2) of the Act of 10 May 2018 on the personal data protection (Journal Of Laws 2019, item 1781) and Article 60(8) 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 (OJ Office EU L 119, 04.05.2016, p. 1, OJ Office EU L 127, 23.5.2018, p. 2 and OJ Office EU L 74, 04.03.2021, p. 35), following the administrative procedure concerning Ms [REDACTED] residing in Poland, [REDACTED] concerning irregularities in the processing of her personal data by [REDACTED], [REDACTED], with its registered office [REDACTED] Luxembourg, consisting of the processing of an e-mail address after the closure of the [REDACTED], the President of the Personal Data Protection Office

decides to discontinue the proceedings.

Justification

The Personal Data Protection Office (hereinafter: UODO) received a complaint from [REDACTED] [REDACTED] residing in Poland, [REDACTED], on irregularities in the processing of her personal data by [REDACTED] with its registered office [REDACTED] Luxembourg (hereinafter: the Company), processing the email address after the closure of the [REDACTED] account.

In the course of the administrative procedure, the President of the UODO established the following facts:

1. The Complainant stated that she had closed her [REDACTED] user account. Following the closure of the account, she received emails concerning the changes of the Terms and Conditions. The Complainant did not request the Company to erase her email address, since, in her view,

contacting [REDACTED] was possible only after logging in to the user account (evidence: Complainant's letter of 05.03.2021).

2. Since [REDACTED] is established in Luxembourg, the President of the UODO, pursuant to Article 4(23) 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 (OJ Office EU L 119, 04.05.2016, p. 1, OJ Office EU L 127, 23.5.2018, p. 2 and OJ Office EU L 74, 04.03.2021, p. (35) (hereinafter: GDPR), identified the cross-border nature of the case and on 08.07.2021, acting on the basis of Article 56(1) GDPR, forwarded a complaint to the Internal Market Information System of the European Commission (hereinafter: IMI) to identify the lead authority of the case and the authorities concerned (evidence: IMI Report A56ID 309483.1).
3. On 17.08.2021, the Luxembourg Supervisory Authority – Commission nationale pour la protection des données (hereinafter: CNPD) recognised itself as the lead supervisory authority in the case (evidence: IMI: LSA-CSA Feedback Report A56ID 309483.1).
4. On 17.08.2021, the CNPD, pursuant to Art. 61 GDPR, created IMI 61VMN notification 317716.1, in which it asked the UODO to provide it with additional information on the case. The CNPD asked for the Complainant's email address, linked to the deleted [REDACTED] account. CNPD also asked for all copies of correspondence between the Complainant and the Company and copies of emails received after the closure of the user's [REDACTED] account. The CNPD indicated that the Complainant had stated in the complaint that she had attempted to intervene directly in the Company, but any contact with the service was possible only after logging into the user account. CNPD pointed out that this information was not true as it was possible to contact the Company by using the online form available after selecting the button 'I cannot log in or I have no account' (evidence: IMI REPORT 61VMN 317716.1).
5. The President of the UODO sent the letter to the Complainant with questions and findings of the CNPD on 27.08.2021. The letter was effectively delivered on 06.09.2021 (evidence: letter from the President of UODO of 27.08.2021 with a the acknowledgement of receipt). The Complainant did not reply to that letter, which was communicated to the CNPD (evidence: IMI REPORT 61VMN 352334.1).
6. On 16.09.2022, the CNPD published a draft decision in the IMI system, dismissing the complaint and indicating that, by derogation of Art. 60(7) GDPR, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof (evidence: A60DD IMI REPORT

438847.1). The President of the UODO agreed with the draft decision in the case (evidence: A60DD Reasoned Objections Report 438847.1).

After examining all the evidence gathered in the case, the President of the UODO considered the following.

Article 60 of the GDPR regulates the cooperation between the lead supervisory authority and the other supervisory authorities concerned. In accordance with Article 60(1) GDPR, the lead supervisory authority cooperate with the other supervisory authorities concerned. The lead supervisory authority and the supervisory authorities concerned exchange all relevant information with each other. According to Article 60(7) GDPR, 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. Art. 60(8) GDPR provides that, by derogation from paragraph 7, where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged shall adopt the decision and notify it to the complainant and shall inform the controller thereof.

In the light of the above, the CNPD, acting as the lead supervisory authority in the case, adopted a draft decision in which it discontinued the proceedings and acting on the basis of Article 60(8) GDPR, sent it to the President of the UODO, as the authority with which the complaint was lodged. Consequently, the President of the UODO adopts a decision in this case.

The President of the UODO, acting on the basis of the Code of Administrative Procedure (Journal of Laws Of Laws 2022, item 2000), hereafter: the KPA assesses, on the basis of all the evidence gathered, whether a given circumstance has been proved. Evidence in proceedings may include, in particular, documents, witness statements, expert opinions and visual inspection (Article 75(1) of the KPA). A public administration body may consider the facts of the case to be determined only on the basis of clear evidence and cannot confine itself to establishing a *prima facie* case unless otherwise provided for in the KPA.

In the present case, the Complainant indicated that she had a [REDACTED] account, which she decided to close, but despite the closure of the account, she received emails concerning changes of the terms of the service. The Complainant also stated that she had attempted to intervene directly with the Company, but in her view, contact with the service was possible only after logging in to the account.

The CNPD, acting in its capacity as the lead supervisory authority in the case, asked the Complainant to provide an e-mail address linked to the closed account, to forward a copy of all correspondence between the Complainant and the Company and a copy of the emails received after the closure of the [REDACTED] account. The CNPD found that the Complainant's claims that it was not possible to contact the Company if she did not have a user account were not correct, since it was possible to contact the Company using the online form available after selecting the button 'I cannot log in or I have no account'.

The President of the UODO sent a request for additional information and findings from the CNPD to the Complainant on 27.08.2021, the letter was effectively delivered to the Complainant on 06.09.2021. The Complainant did not reply to it.

The Polish Supreme Administrative Court in its judgment of 26.10.1984 (ref.: II SA 1205/84, ONSA 1984, No 2, item (98) ruled that: 'It follows from Articles 7 and 77(1) of the Code of Administrative Procedure that the authority conducting the administrative proceedings is required to examine and consider all the evidence gathered exhaustively. This does not mean that a party is exempted from complicity in the implementation of that obligation, especially since failure to prove a particular fact may lead to adverse results for the party.' The Supreme Administrative Court reiterated this position in its judgment of 12.07.2017, ref. II GSK 2757/15, adding that (quote): 'Nor can it be inferred from those provisions that the administrative authorities are required to seek evidence in support of a party's assertions where that party does not itself take the initiative of providing any evidence. In the event of a party's inaction, the authority cannot be expected to prove facts intended to militate against its findings.'

In the present case, the Complainant did not indicate to which e-mail address she received the new messages, nor did she provide any evidence of receipt of such messages or any correspondence with [REDACTED]. At the same time, the lead supervisory authority found that the Complainant's claims that it was not possible to contact the Company in the absence of a user account were not correct, since it is possible to contact the Company using the online form available after selecting the button 'I cannot log in or I have no account'.

In the light of the above, it must be concluded that the investigation carried out did not provide evidence that the Complainant's personal data had been processed in the form of her e-mail address following the deletion of the user's account in [REDACTED]. In addition, no clear evidence was obtained during the proceedings that the Complainant was unable to contact the Company in the absence of a user account.

In accordance with Article 105(1) of the KPA, where proceedings have become devoid of purpose for any reason, the administrative authority shall issue a decision to discontinue the proceedings. The determination by a public authority of the existence of the condition referred to in Article 105(1) of the KPA obliges it, as it is pointed out in doctrine and jurisprudence, to discontinue proceedings, since there are no grounds for issuing a decision on the substance of the case where that condition exists, and the continuation of the proceedings in such a case would amount to a flaw in that case, which would have a significant impact on the outcome of the case.

According to the evidence gathered in the case, there is no proof to support the Complainant's allegations, so that it cannot be considered that the processing of the personal data had taken place, with the result that those proceedings had become devoid of purpose.

In this factual and legal situation, the President of the Personal Data Protection Office decided as set out in the operative part of this decision.

Under the authority of the President
of the Personal Data Protection Office
Director of the Complaints Department



The decision shall be final. Pursuant to Article 7(a) 2 of the Personal Data Protection Act of 10 May 2018 (Journal Of Laws 2019, item 1781) in conjunction with Articles 13(2), 53(1) and 54 of the Proceedings before Administrative Courts Act of 30 August 2002 (Journal of Laws Of Laws 2022, item 329 as amended), a party who is dissatisfied with this decision has the right to lodge a complaint with the Provincial Administrative Court in Warsaw within 30 days of being served on the party. The complaint is lodged via the President of the Personal Data Protection Office (address: Personal Data Protection Office, ul. Stawki 2, 00-193 Warsaw). The entry for the complaint is PLN 200. A party has the right to apply for exemption from court costs or for the right to aid.

Summary Final Decision Art 60 Complaint

Violation identified, No sanction,

EDPBI:AT:OSS:D:2022:357

Background information

Date of final decision:	22 April 2022
Date of broadcast:	22 April 2022
LSA:	AT
CSAs:	DEBW, DEBE, DEHE, DERP, DENI, ES
Legal Reference(s):	Article 44 (General principle for transfers), Article 45 (Transfers with an adequacy decision), Article 46 (Transfers by way of appropriate safeguards), Article 49 (Derogations for specific situations)
Decision:	Violation identified, No sanction
Key words:	International transfer, Profiling, Social media, Advertising, Cookies.

Summary of the Decision

Origin of the case

The controller provides an online comparison portal for consumer products in several Member States and is registered in Austria. On 18 August 2020, the LSA received a complaint against both the controller and the processor (Google LLC) concerning the transfer of the complainant's personal data to the United States of America (US). The personal data were collected during the complainant's visit to the controller's website incorporating the free version of the Google Analytics tool. Such data were collected through the user's HTTP request, browser information and first party cookies. After collection, these data were transferred to Google LLC to generate behavioural analyses.

As safeguards for this data transfer, the controller and Google LLC had implemented several measures. The contractual safeguards included the conclusion of standard contractual clauses whereas the implemented organisational and technical safeguards consisted of, among other things, the publication of transparency reports by Google LLC and the use of an IP anonymisation function.

Findings

Firstly, the LSA noted that it was competent to deal with the complaint at issue in so far as the ePrivacy Directive, which acts as the *lex specialis* of the GDPR according to Article 95 GDPR, does not contain any obligation regarding transfers within the meaning of Chapter V GDPR.

Contrary to the controller's contention, the LSA held, in line with the case law of the CJEU and the wording of Article 77(1) GDPR, that the obligation under Chapter V and, in particular, the one to ensure that the level of protection of individuals guaranteed by the GDPR is not undermined by transfers of personal data, can also be asserted as a subjective right before the competent control authority. Following this, the LSA found that the controller had transferred personal data of the complainant to the US, through Google LLC, by implementing the Google Analytics tool on its website. Considering that the IP addresses of data subjects were anonymised only after the transfer to Google LLC, and Google LLC was subject to the relevant laws of the US granting national intelligence services access to the transferred data regardless of where it stored its data, the LSA concluded that the transfer was an international transfer of personal data within the meaning of **Chapter V GDPR**.

In this respect, the AT SA first found that the transfer could not be covered by **Article 45 GDPR** due to the invalidation of the EU-US adequacy decision by the CJEU (Case C-311/18). The LSA then looked at the safeguards implemented by the controller in accordance with **Article 46 GDPR**. In that respect, the LSA found that the standard contractual clauses adopted between the controller and Google LLC did not provide by themselves an adequate level of protection as required under Article 46 GDPR considering that Google LLC, as an electronic communication supplier, was subject to surveillance law by USA intelligence services. In addition, the LSA found that the supplementary measures implemented to safeguard the transfer were not adequate, since they do not close the legal protection gaps identified in the judgment of the CJEU C-311/18, i.e. the access and monitoring possibilities of US intelligence services. Further, the AT SA noted that no other instrument under Chapter V GDPR was used to ensure an adequate level of protection of the transferred personal data. In the absence of any other tools of transfer, the AT SA found that the controller had not ensured an adequate level of protection as referred to in Article 44 GDPR.

Finally, the LSA pointed out that this finding is not altered by the fact that the controller had ceased from using the Google Analytics tool. Finally, as regard Google LLC's argument that a risk-based approach should be taken when assessing the adequacy of the transfer to the USA, the AT SA recalled that the GDPR includes no such mechanism or principle regarding data transfers.

Decision

In relation to the first complaint against the controller, the LSA found that the controller had breached the general principles of Article 44 GDPR. However, as the controller had stopped transferring data to the US by removing the Google Analytics tool from its website before the conclusion of this case, no suspension order was made by the LSA. In addition, the LSA dismissed the second complaint against Google LLC.

Summary Final Decision Art 60

Complaint

Rejection of complaint

EDPBI:HU:OSS:D:2020:117

Background information

Date of final decision:	25 June 2020
Date of broadcast:	02 July 2020
LSA:	HU
CSAs:	BE, CZ, DE (BE, HB, HE, NI), DK, EE, ES, FR, IT, NO, PT, RO, SE, SK
Legal Reference:	Right to erasure (Article 17) Right to object (Article 21)
Decision:	Rejection of complaint
Key words:	Exercise of the rights of the data subjects, marketing

Summary of the Decision

Origin of the case

The complainant lodged a complaint against the controller with one of the CSAs after receiving unsolicited marketing messages. The complainant requested to unsubscribe on several occasions without success.

Findings

The LSA requested that the complainant make a statement within eight days in order to disclose his identity to the controller in the course of the procedure, warning that without disclosing his identity the investigation could not be conducted. The LSA also requested a copy of the erasure request addressed to the controller, as well as copies of any other communications and correspondence with the controller and the controller's response to the erasure request.

The LSA repeated this request a number of months later as there was no response from the complainant.

In the absence of a response, the LSA examined the documents made available to it by the CSA. It was not possible to establish from the screenshots enclosed when the complainant unsubscribed from the

controller's newsletter or on how many occasions. The documents were not dated and email addresses were not visible or available.

The screenshots of the electronic newsletters of the controller do not reveal the addressee nor the email address that they were sent to.

Decision

As the complainant's request remains unverified, no decision establishing an infringement can be made. The LSA has rejected the complaint without an investigation of merit.



631.47.3

06 July 2020

A56ID 66040
Case Register 72790
DD 103674

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

The complaint is rejected.

Legal basis: Art. 15, Art. 21, Art. 57(1)(f), Art. 60(8) and Art. 77 of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).

REASONS

A. Arguments of the parties and procedure

1. By letter of 14 March 2019, the complainant informed the Berlin DPA that he had been receiving advertising e-mails for months. It was alleged that one could unsubscribe through the infoboxes in these e-mails. In the imprint of an enclosed e-mail message, the controller was named. On the basis of Art. 15 DSGVO, the complainant wanted to know where the controller got his data from, to whom the data was forwarded, what purpose the storage it served and what data about him was stored.
2. Since the facts of the case are based on cross-border data processing, the Berlin DPA placed the case in the Internal Market Information (IMI) system, which is used in the context of the cooperation procedure and consistency mechanism to handle the cross-border procedure in accordance with the provisions of the GDPR. It turned out that the controller's main establishment, per address Wienerbergstraße 111/12A, 1100 Vienna, is Vienna, so that the Austrian data protection authority (DPA) is the lead supervisory authority in this procedure pursuant to Art. 56(1) GDPR.
3. On 5 August 2019, the Austrian DPA requested the Berlin DPA to submit the correspondence of the complainant in which he asserts his rights as a data subject vis-à-vis the controller, since this correspondence had not been enclosed with the original complaint. On 29 October 2019, the Berlin DPA informed the Austrian DPA by way of mutual assistance in the "Internal Market Information (IMI) System", IMI number: A61VM 72872 to the effect that the complainant has not yet acted vis-à-vis the controller and is therefore unable to produce any correspondence.

B. Subject matter of the complaint

In the present case, the question arises whether the respondent infringed the complainant's right to information or his right to object.

C. Findings of the facts

The complainant has received an unsolicited advertising e-mail from the controller. He informed the Berlin DPA of this fact in the context of his complaint of 14 March 2019. The controller has its main establishment in Austria. The complainant did not contact the controller regarding the assertion of his rights as a data subject concerned.

Evaluation of the evidence: The findings result from the complainant's submission to the Berlin DPA dated 14 March 2019 and from the notification of the Berlin DPA to the Austrian DPA in the Internal Market Information (IMI) system dated 29 October 2019.

D. From a legal point of view, it follows:

It follows from Art. 12 GDPR that the rights under Art. 15 to 22 GDPR are rights that require a request by the data subject.

As has been established, in the present case, such requests for information (Art. 15 GDPR) or objections (Art. 21 GDPR) were not made to the controller, which is why the present complaint had to be dismissed for this reason alone.

If a complaint is dismissed or rejected, the supervisory authority to which the complaint was submitted issues the decision in accordance with Art. 60(8) GDPR and notifies it to the complainant and the controller.

Ref. No. DSB-D130.081/0001-DSB/2019

clerk: [REDACTED]

Data protection complaint (erasure)
[REDACTED]

Decision of the data protection authority

D E C I S I O N

S P E E C H

The data protection authority decides on the data protection complaint of [REDACTED] (complainant) of 12.6.2018 against [REDACTED] (respondent) for violation of the right to erasure as follows:

- The complaint is dismissed.

Legal basis: § 24 para. 1 and para. 5 Data Protection Act (DSG), BGBl. I No. 165/1999 as amended; Art. 17, Art. 60 para. 8 and Art. 77 of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR), OJ No. L 119, 4.5.2016, p. 1.

JUSTIFICATION

A. Arguments of the parties and course of proceedings

1. By complaint of 12 June 2018, improved by submission of 27 June 2018, the complainant alleged a violation of the right to erasure and essentially alleged that he had received e-mails from the respondent to his e-mail address [REDACTED] for almost two years now. His extrajudicial and judicial injunctive relief was systematically ignored. In the legally binding default judgment of 18 October 2017, the District Court Innere Stadt Wien had ruled that the respondent had to refrain from sending electronic mail to the complainant for advertising

purposes in the case of any other execution. He therefore applied to the respondent for his e-mail address to be deleted.

2. Since the matter is a cross-border one and the defendant's principal place of business or only place of business is in the United Kingdom, the proceedings were suspended by decision of the data protection authority of 27 September 2018, Ref. No. DSB D130.081/0002-DSB/2018, from 30 August 2018 until it was determined which authority was responsible for the content of the proceedings (lead supervisory authority) or until a decision by a lead supervisory authority or the European Data Protection Committee had been issued.

3. Subsequently, the British data protection authority (ICO) declared itself to be the lead supervisory authority and submitted the complaint to the respondent for comment.

In summary, the respondent informed the UK data protection authority that the e-mail address [REDACTED] used by the complainant for his application had not been set up to receive messages. This had meanwhile been remedied. The postal address used had been out of date, so that the respondent had not received the complainant's letters. In the meantime, the complainant had removed the complainant from the marketing mailing list.

With this in mind, the UK data protection authority stated that the complaint would have to be rejected because of the deletion.

4. The respondent's opinion was transmitted to the complainant during the hearing of the parties. No opinion was received from the complainant within the time limit set.

5. With regard to the decision of the lead supervisory authority, the decision of the data protection authority suspending the proceedings was rectified by today's decision.

B. Subject-matter of the complaint

In the present case, the question arises whether the complainant's right to erasure has been infringed.

C. Establishment of the facts

In the past, the respondent has sent several e-mails to the complainant for advertising purposes.

In the meantime, the respondent has removed the complainant's e-mail address from the marketing mailing list.

Evidence assessment: The findings are based on the submissions of the parties to the proceedings and on the contents of the file.

D. From a legal point of view, it follows:

Pursuant to Art. 17 para. 1 GDPR, a data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if one of the reasons stated in Art. 17 para. 1 GDPR applies.

As can be seen from the findings, the respondent has in the meantime fully complied with the complainant's request and deleted the e-mail address.

The complaint therefore had to be dismissed for lack of complaint.

Pursuant to Art. 60 para. 8 GDPR, the supervisory authority with which the complaint was filed decides if a complaint is rejected or rejected.

LEGAL NOTICE

An appeal against this decision may be lodged in writing with the Federal Administrative Court within four weeks of notification. The complaint must be lodged with the data protection authority and must be

- the name of the contested decision (GZ, subject)
- the name of the authority being prosecuted,
- the grounds on which the allegation of illegality is based,
- desire and
- the information necessary to assess whether the complaint has been lodged in good time, must be included.

The data protection authority may within two months either amend its decision by means of a preliminary decision on the complaint or submit the complaint with the files of the proceedings to the Federal Administrative Court.

The appeal against this decision is subject to a fee. The fixed fee for a corresponding submission including enclosures is 30 euros. The fee is to be paid into the account of the tax office for fees, transaction taxes and gambling [REDACTED]
[REDACTED] whereby the respective appeal procedure (business number of the notice) is to be stated as the purpose of payment on the payment order.

In the case of electronic transfer of the appeal fee with the "tax office payment", the tax office for fees, transaction taxes and gambling (IBAN as before) must be stated or selected as the recipient. In addition, the tax number/tax account number [REDACTED] the tax type ' [REDACTED]
[REDACTED], the date of the notice as the period and the amount must be stated.

The payment of the fee must be proven to the data protection authority when the complaint is lodged by means of a original payment receipt confirmed by a postal office or a credit institution, which must be attached to the submission. If the fee is not paid or not paid in full, a report is sent to the competent tax office.

A timely filed and admissible appeal to the Federal Administrative Court has suspensive effect. The suspensive effect may have been excluded in the ruling of the decision or may have been excluded by a separate decision.

7 March 2019

For the head of the data protection authority:

[REDACTED]

Summary Final Decision Art 60

Complaint

Compliance order to controller

Background information

Date of final decision:	29 January 2019
LSA:	BE
CSAs:	DE (Rhineland-Palatinate), FR
Legal Reference:	Right of Access (Article 15), Right to erasure (Article 17), Transparent information, communication and modalities for the exercise of the rights of the data subjects (Article 12)
Decision:	Compliance order to controller
Key words:	Data subject rights, Right of access, right to erasure, transparency

Summary of the Decision

Origin of the case

The complainant requested that the controller shall grant his right to access and following this, grant the right to erasure. The complainant did not receive any reply at all until the date of the complaint, despite the obligation provided in Article 12.3 GDPR, according to which the controller shall inform the data subject about the follow-up of the request within one month since the receipt thereof.

Findings

So far, the controller has not reacted to the initial request for the exercise of the right of access and the right to erasure.

Decision

The SA issued a data subject rights compliance order to the controller on the Right to Access and following this the Right of Erasure.

Final Decision

Complaint against IQ OPTION EUROPE LTD - Deletion Request

The Office of the Commissioner for Personal Data Protection (hereafter "CY SA") refers to the complaint of Mr. █ (hereafter "the complainant") lodged with the Data Protection Commissioner of Hessen, Germany.

Case description

The complainant was denied erasure of his data due to his earlier consent to the general terms and conditions. The general terms and conditions, however, do not elaborate on the data subjects' rights but only refer in a general manner to the GDPR.

The CY SA requested from IQ OPTION EUROPE LTD, to provide information on:

- a) The purpose of keeping the data of the complainant,
- b) The specific legal grounds of non-compliance with the erasure request of the data subject,
- c) The categories of all the data of the complainant which were not deleted.

CY SA received from IQ OPTION the requested information within the set timeframe.

IQ OPTION response

In its response, IQ OPTION explained that, as a regulated entity they are obliged by the AML national legislation (The Prevention and Suppression of Money Laundering Activities Law of 2007 (Law 188(I)/2007)), specifically provided under section 68 of this law as well as the MiFiD and MiFIR EU regulations, to preserve the data records for a specified retention period (at least 5 years) to ensure that regulators (mainly the Cyprus Securities and Exchange Commission), companies and customers have access to key business records surrounding financial transactions.

They provided a list of all the personal data of the complainant, which were not deleted and for each one of them they indicated the legal basis for keeping those data. The legal basis is either national law 188(I)/2007 indicated above or/ and MiFiD and MiFIR regulations.

With regards to the subject matter of the complaint, IQ OPTION confirmed that, despite the company guidelines, the reply initially provided to the complainant by their support services was indeed incomplete and did not inform the client of the legal grounds obliging IQ OPTION to maintain his data. As a corrective measure, they confirmed that a formal and complete reply was prepared to be sent to the complainant explaining why his personal data cannot be erased due to the legal restraints imposed by the regulator (Cyprus Securities and Exchange Commission) pursuant to Cyprus legislation and confirming that as soon as the date upon which their obligation to maintain the data expires, they will proceed to the removal/erasure of all personal data.

IQ option further emphasised in its letter that it is their priority to effectively deal with all requests received, that they adopted all necessary internal technical and organisational measures imposed by the GDPR and the national laws to be in a position to reply to all demands in a timely manner and will do their very best to avoid having any such issues arise in the future.

Moreover, IQ OPTION affirmed that it has taken additional measures concerning data subject rights/ privacy policy following the complaint:

- All the procedures were reviewed to ensure that data minimisation principle is adequately applied and in particular to ensure that only the absolutely necessary data for the performance of their services are processed and in compliance with the laws and regulations relevant to their activities.
- The DPO planned additional training sessions to the staff interacting with the client, to remind them of the procedures. The DPO further circulated detailed instructions as to how the staff should reply to each type of request, in order to avoid having a similar miscommunication with clients in the future.

Our view

CY SA considers that IQ OPTION provided all the necessary elements related to the complaint.

We verified the list of all the personal data of the complainant, which were not deleted and it appears that for each one of them the legal basis for keeping the data is relevant - either national law 188(I)/2007 or/ and MiFiD and MiFiR regulations – and in compliance with the minimisation principle. We further checked with the Cyprus Securities and Exchange Commission that the categories of data maintained are indeed relevant.

In light of the above, we conclude that the data of the complainant cannot be erased before the expiration of the timeframe provided in the relevant laws due to *lex specialis* principle. We consider that, in this case, the right to erasure does not apply because “the processing is necessary 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” (Article 17(1)(b) of the GDPR).

Based on the above-mentioned explanations, CY SA did not identify any infringements of the obligations set out in the GDPR by IQ Option.

Commissioner
for Personal Data Protection

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	13 June 2019
LSA:	CY
CSAs:	AT, DE-Hessen, DK, ES, FR, NL, NO, SK, SE
Controller:	IQ OPTION EUROPE LTD
Legal Reference:	Right to Erasure (Article 17)
Decision:	No violation
Key words:	Right to erasure, e-commerce, Exercise of the rights of data subjects

Summary of the Decision

Origin of the case

The complainant alleged that he was denied erasure of his data due to his earlier consent to the general terms and conditions. The general terms and conditions, however, do not elaborate on the data subjects' rights but only refer in a general manner to the GDPR.

Findings

After seeking information from the data controller, the LSA found that the controller was regulated by AML national legislation, which requires the retention of data for at least five years to ensure that regulators, companies, and customers have access to key business records regarding financial transactions.

Decision

No violation as the processing was lawful under the provision Art 17(1)(b) GDPR providing that "the processing is necessary 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".



Our ref. 11.17.001.007.188

10 October 2019

HOSTINGER INTERNATIONAL LTD
61 Lordou Vironos Street
6023 Larnaca, Cyprus

Subject: Examination of complaints – exercise of data subjects' rights under the GDPR

Dear [REDACTED]

Further to the exchange of communications between the Commissioner and HOSTINGER concerning two complaints involving HOSTINGER, we would like to bring to your attention the following assessment of the Commissioner.

Complaint lodged in Spain

In July 2018 a complaint was lodged with the Spanish Agency for Data Protection by [REDACTED] regarding HOSTINGER's failure to comply with his erasure request. The data subject requested by e-mail the erasure of his data on 30/05/2018 and 10/07/2018. The emails were sent to es@hostinger.com with copy to gdpr@hostinger.com. HOSTINGER did not react to these requests nor send any other response to the data subject.

Complaint lodged in Germany

While the investigation of the complaint of [REDACTED] by the Commissioner was ongoing, a similar complaint was lodged in January 2019 in Germany by [REDACTED]. The complainant claimed that he sent a data subject access request (SAR) by e-mail to gdpr@hostinger.com on 9 December 2018 and did not receive any reaction from HOSTINGER.

Hostinger's response

In your initial response to the Commissioner regarding the complaint of [REDACTED] you affirmed that you have searched the mentioned mailboxes - es@hostinger.com and gdpr@hostinger.com – and did not find any message from the data subject, that you also searched the spam and trash folders with no results, that you reviewed the chat records and did not find any conversation with the data subject and that you also contacted the Spanish speaking customers support agents of HOSTINGER and they do not remember such request.

You assured that your agreements, policies and processes were reviewed and amended in April 2018, that your staff is well trained and have directions about GDPR requests; you follow GDPR procedures and delete customers' data when requested. In your letter of 30th May, you provided a copy of the register of client deletion requests, which showcases the amount of handled cases. The register of client deletion requests consists of 985 closed issues as of that date.

You confirmed that the reason of non-compliance with the erasure request of the data subject is that you did not find any evidence that a deletion request was received and you further confirmed that henceforth you complied with the erasure request and took all necessary actions to delete from your system all personal data of [REDACTED]

Further to this, in your letter of 30th May you provided explanations regarding proof of the online verification process you carried out, specifically about requests sent by data subjects to the email gdpr@hostinger.com.

Concerning the complaint of [REDACTED] you affirmed that you never received the data subject request, this is the reason he did not receive any response from you. Following the investigation of the Commissioner, you carried out an internal investigation as per above, but no evidence of the SAR was found. You confirmed that following the complaint, you provided the requested information to [REDACTED] and informed him that his e-mail address and other account data shall not be processed for advertising and marketing purposes, including public opinion polling, as per his request.

Commissioner's assessment

In light of the explanations provided and the actions taken by HOSTINGER to address the issues at stake, we do not currently intend to take any regulatory action on these complaints. The Commissioner reserves the right, in the event of any future complaints lodged by data subjects, to use all powers afforded to her by the GDPR and by national Law 125(I)/2018.

We thank you for your cooperation in these matters.

Best regards,

Commissioner
for Personal Data Protection

Summary Final Decision Art 60 Complaint

No ongoing infringement of the GDPR

Background information

Date of final decision:	10 October 2019
LSA:	CY
CSAs:	DE-Rhineland-Palatinate, DK, ES, FR, HU, IT, LT, PL, PT, SE, SK
Controller:	Hostinger International Ltd
Legal Reference:	Right of access (Article 15), Right to object (Article 21)
Decision:	No ongoing infringement of the GDPR
Key words:	Right of access, Right to object, Data subject request, Advertising and marketing purposes

Summary of the Decision

Origin of the case

Two complainants lodged complaints with two CSAs regarding the controller's failure to comply with their requests. The first complainant demanded that his email and other account data would no longer be processed for advertising and marketing purposes. The second complainant aimed at exercising his right of access.

Findings

Through several investigations, the LSA found that the controller never received the data subject requests. However, following the interaction with the LSA, the controller fully complied with the complainants' requests.

Decision

The LSA found that the controller ultimately complied with his obligations under the GDPR. No further action towards the controller was taken.



Our ref. 11.17.001.006.052

10 October 2019

HOSTINGER INTERNATIONAL LTD
61 Lordou Vironos Street
6023 Larnaca, Cyprus

Subject: Examination of complaints – exercise of data subjects' rights under the GDPR

Dear [REDACTED]

Further to the exchange of communications between the Commissioner and HOSTINGER concerning two complaints involving HOSTINGER, we would like to bring to your attention the following assessment of the Commissioner.

Complaint lodged in Spain

In July 2018 a complaint was lodged with the Spanish Agency for Data Protection by [REDACTED] regarding HOSTINGER's failure to comply with his erasure request. The data subject requested by e-mail the erasure of his data on 30/05/2018 and 10/07/2018. The emails were sent to es@hostinger.com with copy to gdpr@hostinger.com. HOSTINGER did not react to these requests nor send any other response to the data subject.

Complaint lodged in Germany

While the investigation of the complaint of [REDACTED] by the Commissioner was ongoing, a similar complaint was lodged in January 2019 in Germany by [REDACTED]. The complainant claimed that he sent a data subject access request (SAR) by e-mail to gdpr@hostinger.com on 9 December 2018 and did not receive any reaction from HOSTINGER.

Hostinger's response

In your initial response to the Commissioner regarding the complaint of [REDACTED] you affirmed that you have searched the mentioned mailboxes - es@hostinger.com and gdpr@hostinger.com – and did not find any message from the data subject, that you also searched the spam and trash folders with no results, that you reviewed the chat records and did not find any conversation with the data subject and that you also contacted the Spanish speaking customers support agents of HOSTINGER and they do not remember such request.

You assured that your agreements, policies and processes were reviewed and amended in April 2018, that your staff is well trained and have directions about GDPR requests; you follow GDPR procedures and delete customers' data when requested. In your letter of 30th May, you provided a copy of the register of client deletion requests, which showcases the amount of handled cases. The register of client deletion requests consists of 985 closed issues as of that date.

You confirmed that the reason of non-compliance with the erasure request of the data subject is that you did not find any evidence that a deletion request was received and you further confirmed that henceforth you complied with the erasure request and took all necessary actions to delete from your system all personal data of [REDACTED]

Further to this, in your letter of 30th May you provided explanations regarding proof of the online verification process you carried out, specifically about requests sent by data subjects to the email gdpr@hostinger.com.

Concerning the complaint of [REDACTED] you affirmed that you never received the data subject request, this is the reason he did not receive any response from you. Following the investigation of the Commissioner, you carried out an internal investigation as per above, but no evidence of the SAR was found. You confirmed that following the complaint, you provided the requested information to [REDACTED] and informed him that his e-mail address and other account data shall not be processed for advertising and marketing purposes, including public opinion polling, as per his request.

Commissioner's assessment

In light of the explanations provided and the actions taken by HOSTINGER to address the issues at stake, we do not currently intend to take any regulatory action on these complaints. The Commissioner reserves the right, in the event of any future complaints lodged by data subjects, to use all powers afforded to her by the GDPR and by national Law 125(I)/2018.

We thank you for your cooperation in these matters.

Best regards,

Commissioner
for Personal Data Protection

Summary Final Decision Art 60 Complaint

No infringement of the GDPR

Background information

Date of final decision:	10 October 2019
LSA:	CY
CSAs:	DE, DK, ES, FR, HU, IT, LT, SK, NO
Controller:	Hostinger International Ltd
Legal Reference:	Right of access (Article 15), Right to erasure (Article 17), Right to object (Article 21)
Decision:	No infringement of the GDPR
Key words:	Right to erasure, Right to object, Data subject request, Advertising and marketing purposes

Summary of the Decision

Origin of the case

Two complainants lodged complaints with two CSAs regarding the controller's failure to comply with their requests. The first complainant demanded that his email and other account data would no longer be processed for advertising and marketing purposes. The second complainant aimed at exercising his right of access.

Findings

Through several investigations, the LSA found that the controller never received the data subject requests. However, following the interaction with the LSA, the controller fully complied with the complainants' requests.

Decision

The LSA found that the controller ultimately complied with his obligations under the GDPR. No further action towards the controller was taken.



Our ref. 11.17.001.006.014

10 October 2019

Data Protection Officer
SEA CHEFS CRUISES LTD
Limassol, Cyprus

Subject: Result of the investigation – complaint of █ against SEA CHEFS CRUISES LTD about an erasure request under the GDPR

Dear Madam,

Further to the exchange of communications between the Commissioner and Sea Chefs Cruises Ltd concerning a complaint involving Sea Chefs Cruises Ltd, we hereby inform you that after assessment the information gathered in relation to this complaint, the Commissioner is of the view that the company did not infringe any provisions of the GDPR.

Case summary

The data subject submitted an erasure request to the company on 13.11.2018, where he was previously employed. On 12.12.2018 the HR Department of the company, replied that some of his data were deleted and some other data will be kept in order:

- (a) To comply with the legal obligation of the company for tax and VAT purposes
- (b) To safeguard the companies legitimate interests in case of legal claims in accordance with the time limits provided for in law 66(I)/2012.

The data subject lodged a complaint to the Commissioner requesting that all data kept by the controller be deleted.

The controller has its headquarters in Cyprus, and therefore the Commissioner for Personal Data Protection (hereafter “the Commissioner”) is acting as the lead authority in this matter.

The Commissioner requested from the company, to provide information on:

- the complete list of all the personal data of the complainant which were not deleted
- the legal basis for keeping each of the data pursuant to article 17 paragraph (3),

The Commissioner received the requested information, within the set timeframe.

Sea Chefs Cruises Ltd response

During the investigation, you provided the following information:

The Company keeps a copy of the employee's contract of employment to which a copy of his passport is attached. You explained that the copy of the passport is kept for data subject identity verification purposes. You further explained that this information is stored on the company's HR System where you maintain crew data and that it is protected by the various security mechanisms, detailed in your reply (Server/Database security, Workstation security and Network/Communication security).

You provided a complete list of all the personal data of the complainant, which were not deleted.

The legal basis to keep personal data provided in the list, is the compliance with legal obligations according to national law: (a) social insurance contributions and social insurance law (Law 59(I)/2010) (b) tax audit and tax records (Law 4/1978) (c) requirement for retention of supporting documents for verification of identity, employment and salary for social insurance, tax and vat investigations (up to 7 years according to national Law 95(I)/2000) and for establishing, exercising or defending legal claims (up to 6 years according to national law 66(I)/2012)

The salary information, employment contract and passport copy will be deleted after expiration of 7 years, from the date of termination of employment.

The company keeps a copy of the Master's Hearing record, containing the Master's Hearing form, Report to Master, Performance Opportunity Log and Shipboard Crew 45-day appraisal, Security Incident Statements for establishing, exercising or defending legal claims. This information on the data subject's dismissal records will be deleted after the expiration of 6 years from the date of termination, which is the expiration of time to initiate legal claims according to national law. This information is necessary in case the data subject initiates legal claims against the employer.

Commissioner's views

After assessment the information gathered, the Commissioner is of the view that the company complied with its data protection obligations in relation to the issues at stake.

In line with Article 17(1)(b) of the GDPR, the right to erasure does not apply in this case because "the processing is necessary 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".

Namely, on the basis of article 30(2) of the law on Assessment and Collection of Taxes (national Law 4/1978) "books and records shall be kept for a period of **at least six years** from the end of the tax year to which they refer, unless the Director of the Tax Authority requests a longer period".

The national Value Added Tax law (national Law 95(I)/2000), obliges every person (natural or legal) who is subject to the VAT, to keep records and evidences of all expenses, including salaries, for **a period of seven years** from the date of the expense (article 5(3) of the law).

Therefore, information such as passport information, employment contract and salary information (including overtime, bonus and vacation payment) shall be kept for a period of seven years.

Article 7(1) of Limitation of Legal Proceedings act (Law 66(I)/2012) allows **a period of six years** from the date on which the grounds of the legal claim is based, to any person who intends to engage in legal proceeding in relation a contract agreement, such as employment contract.

In light of the above, the Commissioner concluded that the data subject's dismissal records should be kept for a period of six years, as the data subject may appeal the decision of the company to the relevant court, six years after the dismissal.

Based on the above-mentioned explanations, the Commissioner did not identify any infringements of the obligations set out in the GDPR by Sea Chefs Cruises Ltd.

Best regards,

Commissioner
for Personal Data Protection

Summary Final Decision Art 60 Complaint

No infringement of the GDPR

Background information

Date of final decision:	10 October 2019
LSA:	CY
CSAs:	DE-Hamburg
Controller:	Seachefs Cruises Ltd
Legal Reference:	Right to erasure (Article 17), Lawfulness of processing (Article 6)
Decision:	No infringement of the GDPR
Key words:	Right to erasure, Data retention, Legal claims, Compliance with a legal obligation

Summary of the Decision

Origin of the case

The complainant submitted an erasure request to the controller, who was his previous employer. The HR department of the controller replied that some of his data (e.g. his passport information, employment contract, salary information and dismissal records) were to be kept in order to comply with national law obligations and be able to exercise or defend legal claims. As a result, the complainant lodged a complaint requesting the deletion of all his data.

Findings

The LSA found that, pursuant to the applicable national social insurance and tax law, the controller was required to keep records of all expenses including salaries. In order to comply with this obligation, the controller was obliged to keep the complainant's passport information, employment contract and salary information. Moreover, according to the national law on statute of limitations, the controller was allowed to keep the complainant's dismissal records for a period of six years after the dismissal as the complainant could appeal the decision of the controller to the relevant court.

Decision

The LSA found no infringement of the GDPR made by the controller.



Final Decision

IMI Article 56 identification of LSA and CSA entry	55239
National file number	11.17.001.006.019
Controller	Marikit Holdings Ltd (22bet.com)

Marikit Holdings Ltd
22bet.com
Nicosia, Cyprus

Dear [REDACTED]

Further to the exchange of communications between the Office of the Commissioner and Marikit Holdings Ltd (22bet.com), concerning a complaints involving 22bet.com, we would like to bring to your attention the following assessment of the Commissioner.

Summary of the Case

The data subject created an account with the controller (22bet.com) in the context of the “Ronaldinho & Friends vs. Adler All Stars” in November 2018. The enrolment was a prerequisite so as to be able to participate to a competition. The data subject tried for days to delete his account and to erase his data on this website, but the website did not provide such opportunity. The data subject further sent an email asking the controller the deletion of his account and to erasure of all his data. The controller did not comply with the erasure request and alternatively proposed to merely block the account for one year.

Investigation by CY SA

Cyprus SA contacted Marikit Holdings in January 2019. In the initial response to the Commissioner the controller alleged that the data subject could not be identified, as it was discovered later, the data subject did not provide the relevant email address used upon registration to 22bet.com.

In the response received from the support team of 22bet.com on 01/08/2019, we were informed that in general the organisation holds data that can be requested by regulatory bodies in Cyprus for a wide range of purposes, including, but not limited to the following:

1. Ascertainment of the fairness of the games offered
2. Identification in accordance to KYC and AML requirements
3. Resolutions of disputes, claims, etc. connected with the games offered

Marikit Holdings further alleged that is not in a position to delete data which it reasonably believe will be requested by the regulatory bodies prior to their request as it may entail penalties and other reprimands. Moreover, Marikit Holdings affirmed that it holds data until reasonably sure that no complaint shall be sent by the user to the regulatory authorities for which it could be called upon to give explanations with supporting evidence.

The controller finally confirmed the data of the specific user were deleted as soon as it was reasonably possible to delete.

Commissioner's view and corrective actions

Regarding the subject matter of the complaint, considering the fact that the controller reacted to the deletion request within the time-frame provided in the GDPR and eventually, the erasure request was granted after verification that the deletion of relevant data would not infringe other legal obligations of the controller, Cyprus SA considers that the investigation proceedings can be concluded and no repressive measures are necessary.

Cyprus SA reviewed 22bet.com privacy policy and found that the information provided therein is not sufficient to facilitate the exercise of data subjects' rights.

The controller is therefore requested to revise its privacy policy of 22bet.com regarding the exercise of the data subjects' rights and bring it in line with the GDPR and inform the Commissioner accordingly.

The Commissioner reserves the right, in the event of any future complaints lodged by data subjects, to use all powers afforded to her by the GDPR and by national Law 125(I)/2018.

Commissioner
for Personal Data Protection

Summary Final Decision Art 60

Complaint

Compliance order

Background information

Date of final decision:	12 November 2019
LSA:	CY
CSAs:	DE-Lower Saxony, DE-Rhineland Palatinate, ES, FR, HU, NO
Controller:	Marikit Holdings Ltd.
Legal Reference:	Right to erasure (Article 17), Information to be provided to the data subject (Articles 13 and 14)
Decision:	Compliance order
Key words:	Right to erasure, Compliance with legal obligations, Data subject rights

Summary of the Decision

Origin of the case

The complainant alleged that after opening an account on the controller's website to participate in a competition, he was not given the possibility to exercise his right to erasure and delete his account. When the complainant contacted the controller to request the erasure of his account, the controller initially replied that deletion was not possible, proposing to block the account for one year instead.

Findings

In its initial reply to the LSA, the controller alleged that the data subject could not be identified as s/he did not provide the relevant email address. Subsequently, the controller informed the LSA that it would retain the data until it would be reasonably sure that such data would not need to be produced as supporting evidence before regulatory bodies, which could request data for a wide range of purposes. The erasure request was eventually granted after verification that deleting the complainant's personal data would not lead to an infringement of other legal obligations.

In addition, the LSA found that the information provided to the data subjects in the privacy policy was insufficient to facilitate the exercise of their rights.

Decision

Since the controller reacted to the erasure request within the timeframe provided in the GDPR and eventually granted it, the LSA found that no corrective measures should be imposed.

Nevertheless, the LSA ordered the controller to revise their privacy policy accordingly and to inform the LSA of the revision.

Final Decision

IMI notification	65835
IMI Case Register	90574
National file number	11.17.001.007.133
Controller	ROYAL FOREX LIMITED (GMO Trading)

Data Protection Officer
Royal Forex Limited
Prodromou & Demetracopoulou 2
4th Floor
1090 Nicosia, Cyprus

Dear Sir,

Further to the exchange of communications between Cyprus SA (the Commissioner for Personal Data Protection) and Royal Forex Limited concerning a complaint involving GMO Trading, we would like to bring to your attention the following assessment of the Commissioner.

Summary of the Case

The data subject had an account with your company and during the period 16/6/18 - 20/6/18 a financial loss incurred. The DS made a complaint to the complaints department of GMO Trading and on 10 July 2018 she was offered a refund of the sum of GBP 3,500 under a settlement agreement and as a gesture of good will. On 17 October 2018 the data subject exercised the right of access under the GDPR requesting "any copy of letters, emails, telephone or text messages you have" in her name. She sent a reminder to complaintsdepartment@gmotrading.com on 16 November 2018 with no result. Finally, she lodged a complaint to the UK Supervisory Authority.

Investigation by CY SA

Cyprus SA contacted Royal Forex Ltd in July 2019. The company explained that the failure to respond to the data subject's request was due to the facts that (a) there has been a change of Directors and Data Protection Officer and therefore the relevant request was misplaced during the handover of open GDPR related enquiries, and (b) once the company received the request it was examining the possibility of interfering into third party data protection rights, while liaising with the clients. Therefore, the company was in communication with external advisors on the matter.

The company affirmed that it eventually complied with the data subject request by email sent to her on the 23 of August, 2019 providing a link to all call recordings between the client and GMO Trading, and a second email on the 17th of September, 2019 providing a link to all communication exchanged between the client and GMO Trading. The second email was sent again since there was a limitation on the link

provided of two weeks (14 days) to be active, and the data subject did not use it during this period.

Commissioner's view and corrective actions

The Commissioner considers that Royal Forex Ltd (GMO Trading) did not comply with data subject's request within the timeframe provided for in the GDPR.

The initial data subject's request was sent on the 17 October 2018. A reminder was sent on 16 November 2018. The data subject's request was complied with a year later and after the data subject has filed an official complaint.

Article 12.3 of the GDPR stipulates that "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."

In this case, the controller did not provide any information on actions taken within one month, nor informed the data subject on the event of complexity, asking an extension of two additional months.

In light of the above, the Commissioner instructs the controller to take all appropriate technical and organisational measures to henceforth comply with the provisions of article 12 of the GDPR and respond to all data subject requests within the timeframes provided for in this article.

The Commissioner reserves the right, in the event of any future complaints lodged by data subjects, to use all powers afforded to her by the GDPR and by national Law 125(I)/2018.

Commissioner
for Personal Data Protection

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

Background information

Date of final decision:	22 January 2020
LSA:	CY
CSAs:	DE-Berlin, DK, ES, FR, PL, UK
Controller:	Royal Forex Limited (GMO Trading)
Legal Reference:	Transparency (Article 12), Right of access (Article 15)
Decision:	Infringement of the GDPR, Order to comply
Key words:	Access request

Summary of the Decision

Origin of the case

The complainant requested to have access to any copy of letters, emails, telephone or text messages she and the controller exchanged. After having receiving no reply, she sent a reminder to the controller. As the controller did not acknowledge this reminder, she lodged a complaint to one of the CSAs.

Findings

The LSA found that the controller complied with the complainant's access request only after a year since the request has been lodged. The controller's failure to provide any information on the actions taken within the timeframe provided by the GDPR was due to the misplacement of the complainants' file during the handover of open GDPR related enquiries. Moreover, the controller had to communicate with external advisors regarding the possible interference of the access request with third party data protection rights, thus delaying further any action.

Decision

The LSA found that the controller did not comply with its obligations under the GDPR and instructed it to adopt appropriate technical and organisational measures to comply with Article 12 GDPR and respond to all data subjects' requests within the timeframe provided for by this Article.



Our ref. 11.17.001.007.125

2 June 2020

[REDACTED]
[REDACTED]
GAIJIN NETWORK LTD
Kyriakou Matsu 10
LILIANA BUILDING, Flat 204
1082 Nicosia, Cyprus

Subject: Investigation of complaint under the GDPR - erasure request of the user [REDACTED]

Dear [REDACTED]

I am writing further to the exchange of communications between GAIJIN NETWORK LTD and my Office, with regard to the data protection complaint that has been raised with the Commissioner for Personal Data Protection (the Commissioner) about how Gaijin has handled an erasure request submitted by the applicant [REDACTED] (the complainant). I hereby inform you of my decision, following the investigation of this complaint.

Your organisation's response

In your initial response of 5 July 2019, you provided the Commissioner with an account of how Gaijin has dealt with this request. You explained that in order to proceed with the erasure request of the complainant, Gaijin needed to identify the applicant and additional information was necessary under these particular circumstances. In accordance with Gaijin internal "Policy for processing personal data rectification and erasure requests" in order to ensure that each erasure request is sent by Gaijin user i.e. the person who registered the game account and has the right to use the account, and not by someone else who received unauthorised access thereto, Gaijin Support Service requests the additional information from the applicant, such as current and previous nicknames, registration date of the account, purchases and DxDiag information. Subsequently, an algorithm is used to identify the user, depending on the extensiveness of answers that will be provided by the applicant.

You then explained the grounds upon which Gaijin based its decision to refuse the erasure request of [REDACTED]. According to your explanations the owner of the account enabled 2-step authentication via email. The applicant stated that he had lost access to the email. In this case, you considered that the applicant should have contacted their email service provider in order to regain access to the email. Gaijin suggested that the applicant add secondary email to the account and asked the applicant to go through the identification procedure in accordance with the internal policies to make sure that the request was sent not by the hacker but by the original owner of the account. The applicant failed to provide any of the information which would enable the authentication.

You affirmed that the current refusal should not be deemed final and that you are willing to erase personal data related to the account as soon as the identification of the data subject is successful.

You further affirmed that you informed the applicant about the refusal, its temporary nature, until the identification procedure is successful and the reasons for your decision.

In your reply of 20.09.2019 you provided to my Office additional documentation/evidence which substantiated your assertions.

Commissioner's view

I have considered the information available to me in relation to this complaint and have the opinion that the erasure request could not be complied with, in this specific case, as far as the complainant did not provide sufficient information which would enable its identification, in accordance with the requirements of Gaijin.

I consider that the identification requirements of Gaijin are justified and in line with article 12.6 of the GDPR. I value that the information requested by the Support Service i.e. current and previous nicknames, registration date of the account, purchases made via the account, game progress etc. is already in possession and processed by the controller. The requirement of Gaijin to provide again this information is therefore considered to be relevant and not excessive in relation to the purpose of the processing and it only aims at identifying the data subject.

Nonetheless, although I recognise that erasure request could not be complied with, within the particular context, you are reminded that according to Article 12.2 of the GDPR the controller is under the obligation to facilitate the exercise of data subject rights. Modalities should be provided for facilitating the exercise of the data subject's rights, including mechanisms to request and obtain, free of charge, in particular, access to and rectification or erasure of personal data (recital 59 of the GDPR).

I consider that the modalities provided in the Policies of Gaijin do not fully comply with the GDPR requirements, and additional modalities should be subsequently implemented, enabling later a data subject with a hacked account to justify his or her identity in accordance with provisions of Article 12.6 GDPR. For instance, **a secret question could be foreseen at registration**.

Action required

In light of the above, and in accordance with the powers conferred to me by Article 58.2.d of the GDPR, you are instructed to bring the processing operations into compliance with the provisions of Article 12.2 of the GDPR, at the latest **within two months** from the date of this letter, and namely to implement another authentication process which could both secure and facilitate the exercise of the data subject's rights.

Commissioner
for Personal Data Protection

Summary Final Decision Art 60

Complaint

Compliance order

EDPBI:CY:OSS:D:2020:109

Background information

Date of final decision: 2 June 2020

Date of broadcast: 2 June 2020

LSA: CY

CSAs: BE, DK, FR, NL, NO, SE, SK

Controller: Gaijin Network Ltd.

Legal Reference: Right to erasure (Article 17)

Decision: Compliance order

Key words: Right to erasure, Identity verification, Data subject rights

Summary of the Decision

Origin of the case

The data subject submitted an erasure request to the controller, which was refused on the ground that the controller could not verify the requestor's identity.

Findings

The controller reported that the account holder had enabled 2-step authentication via email and that individual had stated that he had lost access to the email. The controller suggested that the applicant add a secondary email to the account and asked them to go through the identification procedure to ensure that the request was by the original owner of the account, as per the controller's policy. The applicant failed to provide any of the information that would enable authentication.

The LSA found that the identity verification requirements in the controller's policy for processing personal data rectification and erasure requests were justified and in line with Article 12 (6) GDPR. Namely, the information that could be requested by the controller was already processed by the controller (e.g., current and previous nicknames, registration date of the account and purchases, among others) and was relevant and not excessive in relation to the purpose of the processing, and it

only aimed at identifying the data subject. The policy also provided for the use of an identification algorithm.

The controller informed the data subject that the refusal was temporary and that it would be willing to erase personal data related to the account as soon as the identification of the data subject was successful, together with reasons for that decision. The controller provided the LSA with documentation/evidence that substantiated its assertions.

The LSA considered that the erasure request could not be complied with, in the specific case, as far as the complainant did not provide sufficient information that would enable its identification, in accordance with the controller's requirements. However, the LSA stressed that Article 12 (2) GDPR mandates controllers to provide modalities for facilitating the exercise of data subject rights. The LSA found that the modalities provided in the controller's policy did not fully comply with the GDPR requirements, and additional modalities should be subsequently implemented, enabling later a data subject with a hacked account to justify his or her identity in accordance with provisions of Article 12 (6) GDPR, such as foreseeing a secret question in the registration procedure.

Decision

The LSA instructed the controller to bring the processing operations into compliance with the provisions of Article 12 (2) GDPR, at the latest within two months from the date of the decision, and namely to implement another authentication process which could both secure and facilitate the exercise of the data subject's rights.

THE OFFICE FOR PERSONAL DATA PROTECTION
Pplk. Sochora 27, 170 00 Prague 7, Czech Republic
Phone: +420 234 665 111, Fax: +420 234 665 444
posta@uouu.cz, www.uouu.cz



No. UOUU-07166/18-XX
Prague X March 2019

Inspection report

Supervisory authority:

The Office for Personal Data Protection, with its seat at Pplk. Sochora 27, 170 00 Prague 7, ID 70837627, (hereinafter referred to as 'the Office').

The authority's power to exercise inspection results from Article 58(1)(b) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in conjunction with Section 2 (2) and (3) of Act No 101/2000 on the Protection of Personal Data and on Amendment to Some Acts.

Supervisory staff:

[REDACTED] — the inspector of the Office, inspector's card [REDACTED]
[REDACTED]
[REDACTED]

Inspected party:

[REDACTED], with its registered office at [REDACTED]
[REDACTED], represented by [REDACTED] on basis of Power of Attorney of 8 November 2018,
(hereinafter referred to as [REDACTED]).

Subject of inspection:

The subject of the inspection is compliance with the obligations laid down in Regulation (EU) 2016/679 with regard to the processing of personal data of the customers of [REDACTED] (users of antivirus software, hereinafter 'antivirus SW'), with a focus on the level of protection of the privacy of users of the free version of the antivirus SW with comparison to the paying users.

First inspection act:

Notice on commencement of inspection, No. UOOOU-07166/18-7, delivered on 2 July 2018.

Last inspection act:

Supplemental statement of the inspected party of 30 January 2019, No. UOOU 07166/18-34.

I. Summary of documents:

The inspection report shall be based on the following materials and documents which were collected before and during the inspection and, where appropriate, the documents and information known to the inspection authority from its official activity.

1. Official record of the installation of the free version of the antivirus SW of 25 June 2018, No. UOOU-07166/2018-2, 1 sheet;
2. Official record of the action preceding inspection act of 28 June 2018, No. UOOU-07166/18-6, with annexes:
 - a. a notice on the appointment of the Data Protection Officer of 30 May 2018 (information from the Office's information system), 2 sheets,
 - b. the website's discussion [REDACTED] [REDACTED] (options for setting the privacy level of the [REDACTED] products), 2 sheets;
3. Notice on commencement of the inspection, No. UOOU-07166/18-7, delivered to the [REDACTED] on 2 July 2018, 4 sheets;
4. Reply to the Notice on commencement of inspection and the [REDACTED] statement on the privacy protection level of users of the antivirus SW of 1 August 2018, No. UOOU-07166/18-12, 11 sheets (both the Czech and the English versions);
5. Request of the Office for an oral hearing of 10 August 2018, No. UOOU-07166/18-13, 1 sheet;
6. Requested documents delivered on 21 August 2018, No. UOOU-07166/18-16, 1 sheet, with annexes:
 - a. Assessment of protection, 3 sheets,
 - b. Description of the personal data processing operations, evaluation of needs of data protection impact assessment (PIA), 3 sheets;
7. Record of the oral hearing on 29 August 2018, No. UOOU-07166/18-17, 3 sheets;
8. Request of the Office for an oral hearing of 23 October 2018, No. UOOU-07166/18-22, 1 sheet;

9. Record of the oral hearing on 6 November 2018, No. UOOU-07166/18-25, 2 sheets;
10. Record of the access to the inspection file by the [REDACTED] representative on 14 November 2018, No. UOOU-07166/18-26, including the Power of Attorney, 4 sheets;
11. Statement of the inspected party of 17 December 2018, No. UOOU-07166/18-28, 13 sheets (both the Czech and the English versions);
12. Information concerning the course of the inspection of 16 January 2019, No. UOOU-07166/18-30, 1 sheet;
13. Record of the access to the inspection file by the [REDACTED] representative on 22 January 2019, No. UOOU-07166/18-31, 1 sheet;
14. Official record of the inspection action (materials from the [REDACTED] website) of 28 January 2019, no. UOOU-07166/18-32, 1 sheet, with annexes:
 - a. [REDACTED] Privacy Policy, 15 sheets,
 - b. Compliance with the GDPR — FAQ, 5 sheets;
15. Supplemental statement of the inspected party of 30 January 2019, No. UOOU-07166/18-34, 5 sheets.

II. Inspection findings:

The inspection was initiated based on a complaint filed with the Dutch supervisory authority on 25 May 2018. The complaint concerned the impossibility to de-activate the default privacy protection settings in the free version of the antivirus SW for Apple Mac. Thus, in view of the contents of the complaint, the subject of the inspection was defined as specified above. In the course of the inspection, the subject of the inspection was specified in more detail as an inspection regarding the level of protection of privacy with respect to the users of the free version of the SW in comparison with paying customers, with a focus on the following areas indicated in the complaint:

- a. Processing of personal data of non-paying users of the antivirus SW for marketing activities of the [REDACTED]
- b. Processing of personal data of non-paying users of the antivirus SW for marketing activities of third parties.
- c. Processing of personal data of non-paying users of the antivirus SW for analyses by third parties.
- d. Processing of personal data of non-paying users of the antivirus SW for SW development purposes.

Thus, the inspection is not concerned with the processing of personal data of paying customers of the antivirus SW for the purpose of making and verifying payments. At the same time, the inspection is not limited to the antivirus SW for Apple Mac.

With respect to the definition of the subject of the inspection, it can be stated in general terms that, as a rule, the Office initiates inspections *ex officio*. Even in cases when an inspection is commenced based on a complaint, it is the Office who determines the subject of the inspection – based on the complaint, but not necessarily exclusively within the scope thereof. The above procedure is in accordance with Act No. 255/2012 Coll., Regulation (EU) 2016/679, as well as Act No. 101/2000 Coll., which continues to be applied to procedural issues of the inspections carried out by the Office [until the government draft law on personal data processing (parliamentary press No. 138/0, senate press No. 25) enters into effect].

Furthermore, it must be noted that it is not the purpose of the inspection to precisely describe the technical aspects and functioning of the antivirus SW, but rather to define the nature of the data processed in connection with its installation and use, and subsequently to assess whether the [REDACTED] meets its obligations in the area of data protection.

Inspection finding 1.

The Office primarily assessed whether the information processed by the [REDACTED] in the process of installation of the antivirus SW and its further use constitute personal data in the sense of Art. 4 (1) of Regulation (EU) 2016/679, which 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*". Further, it was assessed whether the data are processed in the sense of Art. 4 (2) of Regulation (EU) 2016/679, which defines processing as "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

First, the inspection verified that at the very beginning of the process of installation of the antivirus SW, the [REDACTED] presents the user with the licence agreement and the language options. Furthermore, basic information is displayed to the user, among others on the privacy level settings in the paid and free version of the antivirus SW. Reference is made to the [REDACTED] Privacy Policy (document No. 14.a) which the user should look up for more detailed information.

The [REDACTED] assigns each installation of the antivirus SW with the "Device ID", i.e. the device identifier used for the installation (download) of the antivirus SW. The Device ID is derived from the technical parameters of the device (e.g. the type of processor, graphics card or motherboard). Furthermore, a randomly generated alphanumeric code, the "Installation ID", is assigned to the installation. The Installation ID is assigned to each individual installation of the antivirus SW. For example, if the antivirus SW is uninstalled from a specific device and then installed again on the same device, each of these installations has the same Device ID, but a different Installation ID. This procedure enables the [REDACTED] to ascertain how many times and in what versions the antivirus SW was installed on the relevant device. In the event of a new installation of the antivirus SW on the same device, the information on the new installation is linked to the information on the original installation through Device ID for the purpose of finding and removing any SW bugs or false positive malware alerts that lead to the uninstallation. The process of generating of the codes does not in any way reflect whether the user selected the paid or free version of the SW (documents Nos. 4 and 7).

Furthermore, the Internet Protocol (IP) address of the relevant device is required for the installation of the antivirus SW. In general terms, IP address can be defined as a series of binary numbers assigned to a specific device for the purpose of its unambiguous identification in

communication within a computer network. The second part of Internet Protocol version 6 (IPv6), the so called “interface identifier”, usually contains a globally unique MAC address of the device. Without the IP address, the device cannot communicate via the internet – it cannot send or receive data. Thus, the IP address can be defined as a unique identifier of a device connected to the internet or local network. For the purpose of installation of the antivirus SW, the [REDACTED] needs to know the IP address of the device. Based on this identifier, the [REDACTED] determines on what device the antivirus SW will be installed (i.e. where the device is located), and the language version. The [REDACTED] stores the IP address of the device for a limited period of time, and subsequently pseudonymises it through hashing or replaces it with less specific location information, e.g. city and country (documents Nos. 4 and 14). According to the statement of the [REDACTED] the pseudonymisation/replacement takes place generally after one month or 60 days.

Following the installation of the antivirus SW, the [REDACTED] collects service data, i.e. information on applications installed on the relevant device, information on files or attachments saved on the device, and information on links to the websites (URL) accessed from the device. This information is necessary for ensuring the functioning of the antivirus SW, i.e. to search for malware and protect the device from malware attacks. If the SW detects unknown or new malware, it sends this information (or a sample of the relevant file) to the [REDACTED]; the report is paired with the Device ID and Installation ID. Consequently, through Device ID and Installation ID, the thus-collected information can be paired with the specific device, or rather the specific installation of the antivirus SW, even retrospectively. The malware samples processed by the [REDACTED] are stored for a de facto unlimited period of time, i.e. during malware detection, prevention and research. Device ID in combination with Installation ID allow the [REDACTED] to determine the scope of the contamination (location of the source or occurrence and speed of the spread of the virus), since based on this information, the [REDACTED] is able to assess the number, type, version and location of the affected devices (documents Nos. 4 and 7).

Within the SW settings (Privacy Settings), the users of both paid and free version of the antivirus SW can choose whether their device will send a sample of the detected malware to the [REDACTED] virus data base, and whether the information obtained from their devices may also be analysed by third parties with whom the [REDACTED] co-operates ([REDACTED]). Furthermore, the users of the paid version have the option to switch off the offers of other products of the [REDACTED] and offers of third-party products ([REDACTED]). At any rate, the offers of third-party products ([REDACTED]) are displayed only in the mobile version of the antivirus SW. Furthermore, the users of the paid version of the antivirus SW may refuse the processing of information for the purpose of development of new products of the [REDACTED].

In mobile devices, the procedure described above differs in that only Installation ID is generated for the purpose of installation, and not Device ID. The process of protection against malware is essentially identical to that on the desktop versions, except that mobile devices update their malware database from the database of the [REDACTED] every day. The users of the paid version of the antivirus SW for mobile devices may disable sending of the detected malware samples for further analysis by the [REDACTED] this option is not available to the users of the free version. Same as in the desktop version, all users of the mobile version may refuse third-party processing of data for the purpose of analysing the use of the application (document No. 7).

It follows from the above that for the installation, as well as for proper functioning of the antivirus SW, it is necessary that the [REDACTED] has the IP address of the device on which the antivirus SW is installed, at least for a limited period of time. The reports sent through the antivirus SW are thus linked to both the Device ID and Installation ID of the device, as well as to the current IP address (until the IP address is replaced by less specific data).

In order to assess whether the [REDACTED] processes personal data of users of the antivirus SW, it is necessary to assess whether the collected information can be attributed to an identified or identifiable natural person. An identified person is an individual whose identity can be directly determined based on the collected information (i.e. a unique identifier such as birth identification number, or a unique combination of identifiers, such as name, surname, address). An identifiable person is an individual who cannot be directly identified from the collected information itself, but whose identity can be determined on the basis of that information (using other available information and means). It also holds that unambiguous identification of an individual does not require determination of the full "civil" identity of the individual; on the internet in particular, unambiguous individualisation of a user based on a certain element can suffice in some cases. For example, based on Recital 26 of Regulation (EU) 2016/679, a natural person is identifiable when means such as singling out can be used. Thus, individualisation may be achieved by pairing data with individual identifiers, such as the IP address, MAC address or other device identifier of a device usually used by individuals. It is typical for the internet that a file containing information on user behaviour, in particular when it contains data collected over a long period of time, may facilitate identification.

In order to assess the nature of information being collected and further used by the [REDACTED] in connection with the provision of the antivirus SW service, it must be noted that Art. 4 (1) of Regulation (EU) 2016/679 expressly states that a natural person can be identified e.g. by reference to an online identifier. Although, being an online identifier, the IP address constitutes primarily a piece of technical information pertaining to the device, it must usually be deemed personal data, in particular when the device is likely owned by a specific individual. Based on Recital 26 of Regulation (EU) 2016/679, account must be taken of all the means reasonably likely to be used by the controller or by another person, if a certain IP address in itself does not enable permanent identification of a device connected to the internet. Thus, the IP address constitutes personal data for anyone who has a feasible and legal possibility to attribute it to specific individuals regardless of who attributes it, or who can reasonably assume that such a possibility can exist. It is thus not decisive whether the individual is directly identifiable, i.e. whether the controller connects the data itself on the basis of the information that is available to it or that it can acquire, or indirectly identifiable, i.e. whether interaction of several entities is necessary for the identification of the individual.

After all, the same conclusions were already reached by the Court of Justice of the European Union (hereinafter the "CJEU") in connection to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Specifically, in judgment of 24 November 2011 in case C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (hereinafter "Scarlet") and in judgment of 19 October 2016 in case C-582/14, Breyer v. Bundesrepublik Deutschland (hereinafter "Breyer").

In the Scarlet case, the CJEU reached the conclusion that for internet service providers, IP addresses are personal data, because they allow the users of devices connected to the internet via IP addresses to be precisely identified. The Breyer case was concerned with the question of whether dynamic IP address constitutes personal data for the online services provider if a third party (an internet service provider, 'ISP') has the additional knowledge required in order to identify the data subject. In this case, the CJEU found that a dynamic IP address as such may be considered personal data even without names linked to it.

Thus, in its case law, the CJEU took an objective approach to the term "personal data" when it stated that dynamic IP address also constitutes personal data if the online services provider has available legal and reasonably usable means enabling identification of a user through a third party (e.g. internet service provider, prosecuting bodies, telecommunications services provider). In the case at hand, reasonably usable means could include the possibility that in certain cases the online services provider may contact the competent governmental authority who, subject to meeting the statutory conditions, may obtain information necessary for the identification of the data subject from a third party. The fact that the online services provider did not have the opportunity to legally obtain supplementary information from the ISP does not change the conclusion that a dynamic IP address constitutes personal data for the online services provider.

The [REDACTED] is not in the position of an ISP that is in all cases able to attribute to the IP address to other identification details of the users of its services. As a provider of a website from which the antivirus SW can be downloaded, the [REDACTED] nevertheless collects the IP address of the device in order to provide for the download and installation of a suitable version of the antivirus SW. The IP address of the device is further necessary to ensure full functionality of the antivirus SW installed on the device.

The [REDACTED] also usually has available means that can be reasonably assumed to be suitable for the identification of a certain individual. In case of public static IP addresses, these means are publicly available information. In case of dynamic IP addresses, the [REDACTED] may contact the competent governmental authority who, subject to meeting the statutory conditions, may obtain information necessary for the identification of the data subject from a third party [in particular under Act No. 127/2005 Coll., on electronic communications and on amendment to certain related laws (the Electronic Communications Act)].

Furthermore, it must be stated that at variance with its statements (e.g. in document No. 4), the [REDACTED] in certain cases most probably has also the identification and contact details of the antivirus SW users, even in case of the free version. This applies in particular in cases where the free version of the antivirus SW is registered via [REDACTED] account or if the user registers in the [REDACTED] (this information is also provided by the [REDACTED] in [REDACTED] Privacy Policy, document No. 14.a). Furthermore, the [REDACTED] is able to identify users who subscribe to the newsletter or provide the [REDACTED] with their identification or contact details, e.g. when using the free trial of the premium antivirus SW.

However, even without the additional information provided in the preceding paragraph, the [REDACTED] has such information (IP address of the device in connection with Installation ID, Device ID and service data) that, in their sum, could facilitate identification of the user.

Based on the above, the Office concluded that in connection with the provision of the antivirus SW service, the [REDACTED] collects data that constitute personal data of users. At the same time, it is clear that the [REDACTED] handles such data in a manner which falls within the definition of personal data processing (i.e. collects, stores, further uses and subsequently destroys the data).

Therefore, in assessing the facts of the matter at hand, the Office concluded that the [REDACTED] **processes personal data** in the sense of Art. 4 (1) and (2) of Regulation (EU) 2016/679.

This conclusion applies to all the versions of the antivirus SW (for the Windows, Apple Mac and Android operating systems), both to paying and non-paying users, since, as described above, the process of installation and subsequent functioning of the antivirus SW is essentially the same. This was also stated by the [REDACTED] in the course of the inspection (documents Nos. 4 and 7). At the same time, it is not decisive whether the [REDACTED] made any partial changes in the settings of the antivirus SW prior to or during the inspection, since the privacy settings of the antivirus SW do not influence the nature of the data collected for its installation and further operation.

The statement of the [REDACTED] that it does not intend to identify users is irrelevant in respect of the legal nature of the data processed by the [REDACTED]. What is important is the factual state, i.e. that the [REDACTED] has data that could lead to identification of users.

However, the above conclusion in itself does not mean that the [REDACTED] is in breach of the rules stipulated by Regulation (EU) 2016/679, since the Regulation presumes that certain activities are impossible without processing the necessary scope of personal data and considers such activities legitimate (subject to meeting certain requirements).

Inspection finding 2.

The Office further assessed whether, when the [REDACTED] processes personal data in connection with the installation and subsequent use of the antivirus SW, it is in the position of a personal data controller in the sense of Art. 4 (7) of Regulation (EU) 2016/679, based on which "*controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

As stated above, in connection with the provision of the antivirus SW, the [REDACTED] collects and further processes data on paying and non-paying users of the product that must be deemed personal data.

By defining the installation procedures and further use and functioning of the antivirus SW, the [REDACTED] also defined the purpose and means of personal data processing. In general, the purpose of the relevant personal data processing may be the business activities of the [REDACTED] and, at the same time, enhanced cyber security of the users. These basic purposes may be further divided into more specific individual purposes, e.g. marketing purposes of the [REDACTED] or third parties, further development of the antivirus SW or analysis by third parties. The

means are the antivirus SW itself, as well as the website [REDACTED] intended for its download. At the same time, the [REDACTED] processes the collected data itself.

Thus, the [REDACTED] is in the position of personal data **controller** in the sense of Art. 4 (7) of Regulation (EU) 2016/679, since it has defined the purpose and means of the relevant processing, carries out the processing itself or through third parties and is responsible for it.

Inspection finding 3.

The Office further assessed whether and to what extent the [REDACTED] fulfils the obligations following from Art. 5 of Regulation (EU) 2016/679, which provides for the basic principles of personal data processing. In view of the course of the inspection, in particular the fact that the [REDACTED] denies that personal data are processed in connection with the installation and operation of the antivirus SW (with the exception of paid users and processing for the purpose of making and verifying payment), the inspectors focused primarily on Art. 5 (2) of the Regulation, which states that the controller "*shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (accountability)*". At the same time, the performance of the obligation imposed on the [REDACTED] by Art. 24 (1) of Regulation (EU) 2016/679 was assessed, i.e. the obligation to implement "*appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*".

As stated above, the inspection established that the [REDACTED] collects and further processes personal data on paying and non-paying users of the antivirus SW it provides. Thus, it is the primary obligation of the [REDACTED] to proceed in compliance with the principles stipulated in Art. 5 (1) of Regulation (EU) 2016/679, and the [REDACTED] is also obliged to document compliance in accordance with Art. 5 (2) and Art. 24 (1) of the Regulation.

Regulation (EU) 2016/679 does not expressly specify the form of documenting compliance, and it is up to each controller to select appropriate measures ensuring compliance with the obligation under the relevant circumstances. In view of the other obligations imposed on controllers by Regulation (EU) 2016/679, it is nevertheless clear that compliance with the basic principles can be documented e.g. by records of processing activities in the sense of Art. 30 of Regulation (EU) 2016/679 or an analysis to evaluate applicability of the individual legal bases, in particular the balance test under Art. 6 (1) (f) of the Regulation, or compliance with approved codes of conduct in the sense of Art. 40 of Regulation (EU) 2016/679 or approved certification mechanisms under Art. 42 of the Regulation.

According to the Office, the obligation stipulated in Art. 24 (1) of Regulation (EU) 2016/679 must be interpreted as the controller's obligation to take into account any and all relevant circumstances surrounding the processing (including the legal basis) and to adopt a set of measures whose goal is to ensure that any and all personal data processing is carried out exclusively under pre-defined conditions that the controller is able to regularly check and enforce if necessary. At the same time, the nature of the measures must be such that they enable the controller to document compliance with the requirements of Regulation (EU) 2016/679. Thus, this obligation supplements the fundamental principle provided for in Art. 5 (2) of the Regulation.

In this context, the Office deems it of fundamental importance that the personal data processing at hand is implemented on a global scale and concerns a considerable number of data subjects. In such a situation, it is absolutely necessary to pay increased attention to all aspects of personal data processing, in particular on lawfulness of the individual purposes of processing and documenting of compliance and other obligations imposed by Regulation (EU) 2016/679, including procedures facilitating exercise of the rights of data subjects.

Nevertheless, the [REDACTED] repeatedly stated during the inspection that it does not process personal data (beyond the scope of the data necessary to make a payment in case of paying users of the antivirus SW). The conclusion made by the inspectors in connection with the nature of the personal data processed by the [REDACTED] on the basis of the arguments provided above was rejected by the [REDACTED] (most recently in its statement of 30 January 2019, document No. 15).

Although, in the course of the inspection, the [REDACTED] provided detailed information on its activities and the installation and basic functioning of the antivirus SW and on the processing of data for secondary purposes (statistics, analyses, further product development, marketing), it failed to document compliance of its processes with the fundamental principles in the sense of Art. 5 (2) of Regulation (EU) 2016/679.

Thus, the inspection was not able to assess compliance with the principles of Art. 5 (1) of Regulation (EU) 2016/679, i.e. in particular what legal basis was defined by the [REDACTED] with respect to all the individual purposes of processing of personal data of the users of the antivirus SW, and whether such legal basis is permissible under the relevant circumstances.

In view of the above, the Office states that the [REDACTED] **breached** the obligations stipulated by Art. 5 (2) and Art. 24 (1) of Regulation (EU) 2016/679.

In connection with this conclusion, the Office states that it is currently pointless to further assess performance of the other individual obligations to which the [REDACTED] is subject as the controller of personal data of the users of the antivirus SW.

III. Cross-border processing of personal data and adoption of decisions

The processing of personal data of users of antivirus SW is a cross-border processing of personal data within the meaning of Article 4(23)(b) of Regulation (EU) 2016/679, as this processing is likely to affect data subjects in more than one Member State. [REDACTED]

[REDACTED] is therefore processing personal data of users from all these countries.

The central administration of [REDACTED] and therefore its main establishment within the meaning of Article 4(16)(a) of Regulation (EU) 2016/679, is located in the Czech Republic. The Office is therefore according to the meaning of Article 56(1) of Regulation (EU) 2016/679 the lead supervisory authority for the processing of personal data within the subject of this inspection. The supervisory authorities of all Member States of the European Union and the European

Economic Area shall be in the position of the concerned supervisory authority pursuant to Article 4(22) of Regulation (EU) 2016/679 in conjunction with the Decision of the EEA joint committee, No 154/2018, of 6 July 2018, amending Annex XI (Electronic communication, audio visual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022].

The Office has provided all relevant information to the concerned supervisory authorities within the meaning of the first sentence of Article 60 (3) of Regulation (EU) 2016/679. The preliminary conclusions were consulted in the informal procedure No A60IC 52303 in the Internal Market Information System ("IMI") from 29 November 2018. On February 8, 2019, a draft decision according to the second sentence of Article 60 (3) of Regulation (EU) 2016/679, was submitted to the supervisory authorities concerned in IMI (procedure A60DD 59825). The draft decision in question was adopted in accordance with Article 60 (4) of Regulation (EU) 2016/679 and as such is binding to the supervisory authorities involved.

Consequently, in accordance with Article 60 (7) of Regulation (EU) 2016/679, members of the inspection team, as persons authorized to act on behalf of the supervisory authority in this case have adopted this decision – inspection report.

IV. Information on right of appeal:

The inspected party may file objections to the inspection findings set out in the inspection report to the inspection authority within a deadline of 15 days from the date of delivering the inspection report. Objections are filed in writing, and it must be obvious which inspection finding they refer to, and must contain a justification of the objection to this inspection finding.

If the inspector does not accommodate the objections within a deadline of 7 days from their delivery, the President of the Office will handle them within a deadline of 30 days from their delivery.

Signature clause:

[REDACTED] Inspector of the Office
.....

[REDACTED] authorized staff member
.....

[REDACTED] authorized staff member
.....

Summary Final Decision Art 60 Complaint

[Violation of Article 24\(1\)](#)

Background information

Date of final decision:	11 July 2019
LSA:	CZ
CSAs:	All
Legal Reference:	Principles relating to processing of personal data (Article 5); Lawfulness of the processing (Article 6); Responsibility of the controller (Article 24)
Decision:	Violation
Key words:	Concept of personal data, Accountability, Consumers

Summary of the Decision

Origin of the case

A complaint was filed with the Dutch SA concerning the processing of personal data of the users of the antivirus software provided by the controller, and specifically the protection granted to users of the free version of the software compared to that granted to the paying users.

Findings

In its inspection report, the LSA concluded that the inspected party failed to comply with Articles 5(2) and 24(1) GDPR, which was interpreted as the obligation to take into account all relevant circumstances surrounding the processing and to adopt a set of measures to ensure that all personal data processing is carried out exclusively under pre-defined conditions that the controller is able to regularly check and enforce. This stemmed from the conclusion that the inspected party, despite its assertions to the contrary, was indeed processing personal data (e.g. IP addresses), based on the Court of Justice case law, and was acting as a data controller.

The controller filed several objections to the inspection report, arguing *inter alia* that no processing of personal data was involved, that it was not to be universally considered as a data controller, and that sufficient information to properly show compliance with Articles 5(2) and 24(1) GDPR was provided. The last objection was partially accommodated by the LSA, which concluded that only an infringement

of Article 24(1) GDPR had been ascertained, whereas no specific breach of Article 5(2) followed from the documentation.

Decision

The controller was found to have violated Article 24(1) GDPR.

THE OFFICE FOR PERSONAL DATA PROTECTION
Pplk. Sochora 27, 170 00 Prague 7
tel.: 234 665 111, fax: 234 665 444
posta@uouu.cz, www.uouu.cz



Ref. No UOOU-02351/19-19
Prague 26. August 2019



IDDS: xwgci53

Request for compliance and reprimand regarding infringement

Let me inform you that following the investigation regarding the complaint received by the Office for Personal Data Protection (hereinafter ‘the Office’) from a German supervisory authority on 13 May 2019, and after assessment of the case at hand, the Office concluded that in this case it is not reasonable to initiate an inspection or administrative proceedings (to impose measures to rectify the infringement).

However, it should be reiterated that by disclosing personal data to another customer’s you have infringed the obligations referred to in Article 32 of the Regulation of the European Parliament and of the Council (EU) 2016/679 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). Furthermore, you have breached this regulation also by failing to evaluate this breach of confidentiality of personal data as personal data breach [REDACTED] the meaning of Article 33 of Regulation (EU) 2016/679, although it is evident that [REDACTED] employees were aware of the breach (as is clear from the e-mail communication between customer and [REDACTED] employee attached to the complaint).

However, in this case there are mitigating circumstances, especially the fact that disclosure of personal data to an unauthorised person was an isolated incident that was clearly attributable to a misconduct of a particular employee, i.e. there are no grounds for suspecting systematic failure to comply with personal data protection obligations. At the same time, following the request made by the Office, [REDACTED] took an immediate action to prevent recurrence of similar security breaches.

Similarly, the absence of an assessment of the breach is due to the misconduct of a specific employee, since the persons responsible for the agenda did not have any information about the breach until they were contacted by the Office. In this context, a mitigating circumstance is in particular the fact that the company had adopted an internal procedure for reporting and notifying personal data breaches, comprising of individual steps to be taken, after awareness of such breach is acquired (handling the incident, documentation regarding the incident, corrective measures), and which includes a method of risk assessment and notification of a breach. Employees are obliged to follow this procedure.

In addition to the above, the fact that [REDACTED] after a request from the Office has willingly cooperated with the Office to resolve the case and has immediately taken steps to resolve the incident, has sent an apology to the complainant and begun realization of measures ensuring such incident does not recur in the future.

In view of the above, and in particular the fact that [REDACTED] based on the Office's request has already taken measures to increase the level of personal data protection, the Office in this case does not consider it to be justified to impose measures to rectify the infringement or to conduct further proceeding.

In this context, I reiterate that controllers must take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. When providing access to personal data (for example [REDACTED]) is then necessary to take measures to verify that the recipient is the intended and authorized person. The level of verification depends on the extent of risk potentially caused by disclosure to an unauthorised person.

In the case of a personal data breach, the controller is obligated to respond to this incident immediately after he becomes aware of it. According to the Office the moment of controller's awareness is inferred from the time when the first person whose conduct is attributable to him became aware of the breach (in this case, it was the customer support officer), irrespective of whether it is such person's job to handle the breaches. If dealing with breaches is not in the job description of the person who has acquired knowledge about the data breach, the controller has to ensure that this information is immediately shared with the responsible person.

Each data breach must be documented and investigated, it must be assessed whether the obligation to notify it to the supervisory authority (within 72 hours from the awareness of the incident) and to communicate it to affected data subjects arose. Regarding the personal data breaches, I recommend to your attention the Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01, adopted by the European data protection board and available on the website https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

Please note, that the case is recorded by the Office and the information [REDACTED] that file might be taken by the Office into account during any future proceedings with [REDACTED] and during the preparation of an investigation plan.

This case was subject to the cooperation procedure according to Art. 60 of the regulation (EU) 2016/679, whereas the Office was the leading supervisory authority.

[REDACTED]
inspector of the Office

Summary Final Decision Art 60

Complaint

Reprimand to controller

Background information

Date of final decision:	26 August 2019
LSA:	CZ
CSAs:	All SAs
Legal Reference:	Security of processing (Article 32), Notification of a personal data breach to the supervisory authority (Article 33)
Decision:	Reprimand to controller
Key words:	Data breach, Request for compliance, Mitigating circumstances

Summary of the Decision

Origin of the case

The complainant, a website's user, alleged that access to their personal information had been disclosed to another user.

Findings

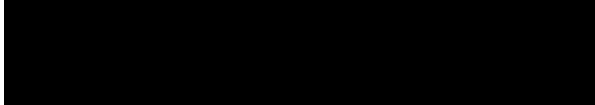
The LSA found that there had been a data breach because a customer support officer accidentally copied the link to a complainant's reservation and sent it to another customer. The controller therefore infringed the obligation to adopt appropriate security measures under art. 32 GDPR as well as the obligations set out by art. 33 GDPR in connection with data breaches. This incident had not been reported by the customer support officer in charge, contrary to the website owner's internal regulations.

After the controller received the LSA's communication, they investigated the incident and began adapting their technical and organisational measures in place and making new ones.

Decision

Also on the basis of the objections received, the LSA decided that although there had been an infringement by the controller of Articles 32 and 33, the imposition of a fine would not have been reasonable, given the mitigating circumstances, especially in connection to the fact that the isolated

incident occurred as a result of a particular employee's misconduct rather than of systemic non-compliance. Therefore, no sanctions were imposed, but a request for compliance and reprimand regarding infringement was sent to the controller.



Ref No. UOOU-03390/19-7

ORDER

The Office for Personal Data Protection, as the competent administrative authority pursuant to Article 58 (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and Section 60 of Act No. 110/2019 Coll., on the personal data processing, decided on 7. October [REDACTED], in line with Section 150(1) of Act No. 500/2004 Coll., the Code of Administrative Procedure, as follows:

Party to the proceedings: [REDACTED] a company with its registered seat at [REDACTED], has been imposed, in connection with the processing of the personal data of debtors, specifically the publication of such data on the website [REDACTED] or on the website [REDACTED] the following obligation:

- I. To cease processing the [REDACTED] personal data in the form of the publication of such data, and remove the already published personal data,
within ten business days of this order entering into force.

- II. To submit to the Office for Personal Data Protection a report on fulfilment of the imposed measure specified in point I of the operative part hereof,
within five business days of the date of fulfilment of this imposed obligation.

Reasoning

The documents collected by the administrative authority when compiling File No. UOOU-03390/19, comprising in particular the documents collected by the Slovenian Supervisory Authority and the materials obtained by the Office for Personal Data Protection (the “Office”), in line with Section 3 of Act No. 255/2012 Coll., form the basis for issuing this order.

On 5 July 2019, in the Internal Market Information System (“IMI”), the Slovenian supervisory authority proposed that the Office be the lead supervisory authority pursuant to Article 56 of Regulation (EU) 2016/679 (procedure A56ID 71098) for the respective processing. On 22 July 2019, the Office accepted the role of lead supervisory authority.

The administrative authority bases point I of the operative part hereof, by which the party to the proceedings is imposed the obligation to cease processing the personal data of the [REDACTED] of the party to the proceedings in the form of the publication of such data, particularly via the website [REDACTED] or the website [REDACTED] and arrange for the removal of the personal data that has already been published, on the facts set out below.

The operator of the [REDACTED] is the party to the proceedings, [REDACTED] a company with its registered seat at [REDACTED] registered in the Commercial Register maintained by the [REDACTED] the executive officer of which is [REDACTED] born DD Month YYYY, residing at Address Number, Post Code, Town (according to the findings of the Slovenian supervisory authority, he was living at the time in [REDACTED], with the company's line of business being the lease of real estate, flats and commercial premises, and production, sale and services not listed in Annexes 1-3 of the Trade Licencing Act (see Ref. No. UOOU-03390/19-3 in this respect). Specifically, the party to the proceedings is involved in [REDACTED] (see Ref. No. UOOU-03390/19-3 in this respect).

The subject-matter of these proceedings is the fact that the party to the proceedings publishes, in addition to its own advertising, the personal data of debtors on its [REDACTED] in the extent of the first letter of each debtor's first name and entire last name as well as the amount of the debt in the currency of the EU, e.g.: dolžnik N. Surname, 43000,-€; dolžnik N. Surname, 23000,-€.

It is clear from the file documents that the described actions of the party to the proceedings has resulted in the publication of information about natural persons, i.e., personal data in accordance with the definition set out in Article 4(1) of Regulation (EU) 2016/679. Pursuant to this provision, personal data is understood as any information relating to an identified or identifiable natural person ('data subject'). Although the party to the proceedings does not publish all of the [REDACTED] identification data, it is clear to the Office that the persons listed here may be directly or indirectly identified based on the published information. In this context, it should be added that in the situation where the identity of a specific natural person is known, it is necessary to consider any other information that can be linked to this person (e.g., debt amount) to be personal data.

As already mentioned, the party to the proceedings publishes on its [REDACTED] the personal data of [REDACTED] in the extent of an abbreviated first name and the entire surname as well as the person's status as a [REDACTED]. The party to the proceedings possesses the respective information due to its business activities:

The party to the proceedings thus publishes through its internet [REDACTED] information about specific cases where it is the [REDACTED] or, more precisely, [REDACTED]. The administrative authority thus considers it proven that the party to the proceedings is, in relation to such information, the personal data controller in accordance with Article 4(7) of Regulation (EU) 2016/679, as within its business operations it determines the purpose and

means of the respective personal data processing. Therefore, the party to the proceedings is subject to all the obligations that stem from Regulation (EU) 2016/679 based on this status.

The basic obligation of personal data controllers is for them to have legal title to process personal data in accordance with the requirements expressed in Article 6(1) of Regulation (EU) 2016/679. With regard to the nature of the respective processing, it is the opinion of the administrative authority that only the legal title of consent under Article 6(1)(a) of Regulation (EU) 2016/679 could generally be applicable. It stems from the file documents, however, that the complainants, as the affected entities, called attention to the fact that the personal data was published despite not having given consent to such publication (see Ref. No. UOOU-03390/19-1 in this respect). For the sake of completeness, the administrative authority states that consent, if granted, should fulfil the requirements placed on informed consent pursuant to Article 7 of Regulation (EU) 2016/679. In similar situations, it is, however, with regard to the degree of interference with the data subjects' rights, highly unlikely that such consent – which is, in particular, free and unconditional and clearly distinguishable from other information – would be obtained.

For the sake of completeness, the administrative authority states in relation to the legal title of legitimate interests under Article 6(1)(f) of Regulation (EU) 2016/679 that not even this legal title applies to the party to the proceedings. Processing based on this legal title must be necessary for the purposes of the legitimate interests of the respective controller or third party; furthermore, the condition that the cases in question are not those where the interests or basic rights and freedoms of the data subjects (requiring the protection of privacy and personal data) take precedence over these interests must be fulfilled. The controller's legitimate interests must first be lawful, i.e., in compliance with legal regulations, and clearly formulated (not speculative). The controller's legitimate interests also include economic interests, i.e., interest in securing the economic side of its business operations. The party to the proceedings in such case could claim and demonstrate legitimate interests (e.g., more effective debt collection or marketing). The publication of the [REDACTED] including the outstanding amount, could explain the [REDACTED] to the proceedings to potential customers, i.e., the seller of the debt, and could force the debtor, through public defamation, to settle the debt. The controller's legitimate interests are, however, insufficient to allow the application of Article 6(1)(f) of Regulation (EU) 2016/679.

In considering legitimate interests, it is also necessary to assess whether the respective processing is necessary to fulfil these legitimate interests, i.e., whether it is not possible to achieve the same result by processing a narrower scope of personal data or infringing to a lesser degree on the data subjects' rights. Besides, minimisation of data is a basic principle of personal data processing and is currently expressed in Article 5(1)(c) of Regulation (EU) 2016/679. In countries where the rule of law applies, [REDACTED] just, however, be carried out in a way foreseen by law and not by public denunciation of the debtors. The party to the proceedings thus has other means at its disposal that would allow it to fulfil its legitimate interest and infringe less on the data subjects' rights. In the administrative authority's opinion, processing in this form is not necessary to attain the controller's or third parties' legitimate interests.

For the sake of completeness, the administrative authority states that if the respective processing indeed was necessary to achieve the legitimate interests, in the context of balancing the interests it would be necessary to balance whether the data subjects' interests

and basic rights prevail over the controller's legitimate interests. In doing so, it would be necessary to take into account the nature and importance of the controller's legitimate interests, the impact of the respective processing on the data subjects, including the data subjects' reasonable expectations, and any other protective measures applied by the controller. The degree of interference with the data subjects' rights is then dependent on the nature of the published information (i.e., [REDACTED] and on the content of this information [REDACTED]. Publication of information about a specific person being [REDACTED] does, however, represent a significant risk in the form of an adverse impact on the rights of these persons in both their personal life and work life. Such information can lead to social exclusion of such persons and their family members, loss of employment and other negative implications. Publication of negative information [REDACTED] of a person thus constitutes such an infringement of the data subject's rights that the simple fact that the respective data subject [REDACTED] [REDACTED] do not justify such processing. The [REDACTED] is not authorised to publish a [REDACTED] personal data each time a [REDACTED]. In this respect, it is necessary, in line with recital 47 of the Regulation (EU) 2016/679, to also take into account the data subjects' reasonable expectations stemming from the fact that the information being published by the party to the proceedings is usually information that is not disclosed. It is in the administrative authority's opinion that the respective processing is not foreseeable by the data subjects. Infringement of the data subjects' rights is also heightened by the fact that publication of information on the publication on the Facebook profile of the party to the proceedings is clearly not limited in time in any way (or it is apparently limited only at the discretion of the party to the proceedings). Moreover, over time, the intensity of the infringement of the data subjects' rights continues to increase. The administrative authority is thus of the opinion that under the same facts, the interests of the controller or any third parties would also be outweighed by the data subject's interests and basic rights and freedoms requiring protection of personal data.

After the summary assessment of the above facts, the administrative authority states that in the case of the systematic publication of information about [REDACTED] under the same circumstances, the interests of the controller or any third parties are generally outweighed by the rights of the affected [REDACTED]. For such processing, the legal title of legitimate interests under Article 6(1)(f) of Regulation (EU) 2016/679 cannot be claimed by the controller.

Based on the collected documents and publicly available information, the administrative authority has sufficient supporting material to assess the legitimacy and legality of the respective actions of the party to the proceedings. As mentioned above, the legal titles under Article 6 of Regulation (EU) 2016/79 cannot be applied to the processing being carried out by the party to the proceedings, and the party to the proceedings has thus breached the controller's obligations stemming from Regulation (EU) 2016/679 in relation to the debtors' personal data.

Based on the above-described complaints and other supporting materials collected from publicly available sources, the Office has reached the conclusion that in the case at hand, there is no reason to commence an inspection pursuant to Act No. 255/2012 Coll., as all of the significant facts and circumstances of the personal data processing have been ascertained in this matter and conducting an inspection at the party to the proceedings would not lead to a collection of other supporting materials essential for assessing compliance of the processing with the requirements of Regulation (EU) 2016/679. A breach of the obligations stemming

from Article 6 of Regulation (EU) 2016/679 was ascertained in the way described above; and, therefore, it is possible in compliance with Article 58(2) of Regulation (EU) 2016/679 and Section 60 of Act No. 100/2019 Coll., to impose the action to remedy the deficiencies identified and set out a deadline for doing so.

Due to the absence of a legal title, it is necessary to cease immediately the processing of the [REDACTED] personal data for the purpose of publishing such data and to remove the personal data that has already been published. The administrative authority is of the opinion that ceasing the processing of personal data without legal title and securing the published personal data are not tasks that require the stipulation of a longer deadline. For this reason, the administrative authority has decided in the way set out in point I of the operative part hereof.

With regard to point II of the operative part hereof, by which the administrative authority imposed on the party to the proceedings the obligation to inform the administrative authority about fulfilment of the measure to remedy the deficiencies specified in point I of the operative part hereof, the administrative authority states that it considers the stipulated deadline of five business days to be reasonable, as providing information about the adoption of measures to remedy the deficiencies is a simple task that is not time demanding.

In accordance with Section 150(1) of the Code of Administrative Procedure, the administrative authority considers the ascertained facts to be sufficient to impose the measure on the party to the proceedings to remedy the ascertained deficiencies in the extent set out in the operative part hereof.

Cross-border processing of personal data and adoption of a decision

Personal data processing carried out by the party to the proceedings is, in accordance with Article 4(23)(b) of Regulation (EU) 2016/679, cross-border processing, as it is likely that the data subjects of more than one EU Member State will be affected by such processing, specifically the data subjects in those countries where the party to the proceedings provides its services.

The inspected party's main establishment in accordance with Article 4(16)(a) of Regulation (EU) 2016/679 is, in relation to the processing that is the subject of the proceedings, i.e., the processing of data subjects' personal data for the purpose of publication thereof, is located in the Czech Republic, [REDACTED]

[REDACTED] The Office is thus the lead supervisory authority in accordance with Article 56(1) of Regulation (EU) 2016/679 for the personal data processing within the subject of the proceedings.

Of the countries of the European Union and the European Economic Area, the party to the proceedings provides its services in the [REDACTED] [REDACTED] (see Ref. No. UOOU-03390/19-1 and Ref No. UOOU-03390/19-3 in this respect). The supervisory authorities of these European Union Member States are, therefore, in the position of the supervisory authorities concerned pursuant to Article 4(22) of Regulation (EU) 2016/679.

In accordance with the first sentence of Article 60(3) of Regulation (EU) 2016/697, the Office has provided the supervisory authorities concerned with all relevant information. In line with the second sentence of Article 60(3) of Regulation (EU) 2016/697, the draft decision was

submitted to the supervisory authorities concerned via the IMI system (procedure A60DD) on 22. August 2019.

The respective draft decision was approved in line with Article 60(6) of Regulation (EU) 2016/679 and as such is binding for the involved supervisory authorities.

With regard to the above and in line with Article 60(7) of Regulation (EU) 2016/679, it was decided as is set out in the operative part hereof.

Information: In line with Section 150(3) of the Code of Administrative Procedure, an appeal against this order can be lodged with the Office for Personal Data Protection within eight days of its delivery, by which the order shall be cancelled and the proceedings made to continue.

This order shall be deemed delivered on the day that its copy is received, but no later than on the tenth day of its being handed over to the postal services operator for delivery. In the event of delivery to a data box, the order shall be deemed delivered at the moment the authorised person logs in to the data box, but no later than on the tenth day of its delivery to the data box.

Prague, 7. October 2019



Inspector

Summary Final Decision Art 60

Complaint

Compliance order

Background information

Date of final decision: 7 October 2019

LSA: CZ

CSAs: AT, DE-All, HR, SI, SK

Legal Reference: Lawfulness of the processing (Article 6)

Decision: Order to the controller, Infringement of the GDPR

Key words: Lawfulness of processing, Legitimate interest, Data subject rights

Summary of the Decision

Origin of the case

The data subjects filed a complaint with one of the CSAs alleging that the controller published his personal data on its social media page without a legal basis.

Findings

The controller published on its social media page information concerning the complainant and other data subjects, referring to debts which the controller was in charge of collecting. The abbreviated first name and the entire surname of the data subjects, as well as the status of debtor and the amount owed by them were specified. Through a balancing test between the data subjects' interests and basic rights with the controller's interests, it was concluded that the controller did not rely on any lawful basis pursuant to Art. 6 GDPR. More specifically, the data subject had not expressed his/her consent; moreover, in the balancing between the legitimate interest pursued by the controller and the interests and rights of the data subject, the latter prevailed, given the significant risk of adverse impact arising from the publication of negative information about the data subjects' financial situation.

Decision

The LSA ordered the controller to cease processing the complainant's personal data and to remove the published personal data within ten business days of the decision. The LSA also ordered the controller to submit a report to LSA on the implementation of the order within five business days of its completion.

Summary Final Decision Art 60

Complaint

No infringement of the GDPR

Background information

Date of final decision:	3 September 2019
LSA:	DE-Berlin
CSAs:	AT, BE, CY, DE-Lower Saxony, DE-Saarland, DK, ES, FI, FR, HU, IT, NO, PL, SK
Controller:	MZ Denmark GmbH (Mozilla)
Legal Reference:	Transparency (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), Right of access (Article 15)
Decision:	No infringement of the GDPR
Key words:	Right of access, Transparency and Information

Summary of the Decision

Origin of the case

The complainant requested to have access to his information without having to send a postal request to the controller's address in the United States. No other contact options such as an email address or web form were listed in the controller's privacy policy.

Findings

The controller communicated to the LSA that, due to a human error, the email address was not included in the privacy policy. This error was immediately rectified following the correspondence with the LSA. The controller also created a portal for enquiries from data subjects. A link to this portal was integrated in the privacy policy.

Decision

The LSA did not find it necessary to establish whether an infringement had taken place, as the controller had complied with his obligations under the GDPR.

Furthermore, the LSA was informed by the SA receiving the complaint that the complainant had withdrawn his complaint.



631.36 / 535.525

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

A hacker attack occurred on the member platform of the European Young Parliament, which is operated by the company CB.e AG on a contract basis. The attacker created 20 fake user accounts and published posts containing malicious code that were publicly accessible to platform users. This is how the malicious code was disseminated. The malicious code carried out a cross-site scripting attack (XSS) whenever a user displayed such a post, which essentially enabled other users' sessions to be taken over and part of their profile data being accessed (e.g. posts and comments on forum and event pages); not, however, the profile data itself, which remained accessible only to the users. In fact, it was discovered that the malicious code only caused redirects to third party websites.

Security measures taken by the data controller when the incident occurred / Specific technical and organizational measures taken by the data controller to combat data breaches

A number of software components have since been updated to current versions. Furthermore, an additional filter has been integrated to prevent cross-site scripting. All active sessions were closed and users have since been prompted to change their passwords, which must now comply with stricter rules. In addition, texts uploaded by platform users are now automatically checked; according to CB.e, manual checks of platform activity are also carried out on a regular basis. Of course, the contributions made by the 20 fake user accounts that contained the malicious code have also been removed.

Analysis of the effectiveness of these measures, particularly regarding the ability to avoid similar data breaches in future

Further XSS attacks should be effectively prevented by the user-generated content being filtered before it is published. Possibly still active user sessions that might have been taken over by the attackers have since been

closed. Implementing stricter password rules and prompting users to change passwords was a generally sensible security measure. It is assessed that the attacker was unable to access or change the password. A second reported data breach comprised an unauthorized access to the e-mail inbox belonging to the e-mail account info@eyp.org using valid credentials. Fewer than 500 e-mails containing malware were sent. A connection to the first data breach was suspected by the responsible party, but this is not assessed as very likely. Instead, it is more likely that the access password for the aforementioned e-mail account was either guessed or, for example, collected using a Trojan on the client PC used for an authorized login. In my opinion, further inquiries into the cause of the breach would not yield any new findings, since the responsible party has no further information to share/provide.

According to the responsible party, in addition to changing the access password to the e-mail account, a switch to a 2-factor authentication system was implemented. In our opinion, this ensures that unauthorized access to the e-mail account is excluded in the future to a reasonable degree.

Summary Final Decision Art 60

Data Breach Notification

No Infringement of the GDPR

Background information

Date of final decision:	17 December 2019
LSA:	DE-Berlin
CSAs:	BE, DE-Rhineland-Palatinate, DE-Saarland, DE-Lower Saxony, DK, ES, FR, HU, LU, NO, SE, SK DE-Berlin
Controller:	Schwarzkopf-Stiftung Junges Europa
Legal Reference:	Personal Data Breach (Articles 33 and 34)
Decision:	No infringement of the GDPR
Key words:	Personal data breach, Hacker attack

Summary of the Decision

Origin of the case

One of the controller's member platforms was attacked by a malicious code, which enabled unauthorised redirect to third party websites. The controller immediately asked the processor to inactivate the platform.

Findings

The LSA found that appropriate security measures, such as the update of number of software components and the request to change users' passwords, were taken by the controller after the incident. Additionally, specific technical and organisational measures were undertaken by the controller to remedy the data breach. Such measures included the automatic check of the content uploaded by users, as well as regular manual check of the platform activity. The LSA found that all the security measures were appropriate. Additionally, the LSA found that a second data breach that followed did not occur because of inadequate security measures and that data breaches in the future could be avoided to a reasonable degree, based on these measures.

Decision

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



Berlin, 19 February 2020

521.10846
631.137
IMI CR 73122
DD 102720
FD 110629

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

To
Sandbox Interactive GmbH
Pappelallee 78-79
10437 Berlin

Reprimand

Complainant: Mr.

Your letter dated 12th March 2019 and 16th October 2019

Dear Mr. ,

We are hereby issuing a reprimand to your company regarding a violation of the General Data Protection Regulation (GDPR) when processing personal data within your scope of responsibility.

Justification:

Our decision is based on the considerations stated below:

I.

We have established the facts as follows:

On 9th April 2016, the complainant purchased the computer game 'Albion Online' from your company, and created a user account. On 24th January 2019 he addressed an email to you with instructions to delete his account in full. The complainant made his request via the support area of the account management section after logging in using his saved registration data.

On 27th January 2019, he was asked to provide additional information, as your company wanted to ensure that the complainant was in fact the owner of the account.

In response to our request for your comments, you explained that a verification of identity was required to prevent an irreparable deletion of a player account, and that the damage would be extensive if the deletion was unauthorised.

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

Following our statement that, under Art. 12 (6) GDPR, the controller may only request additional information should reasonable doubt arise regarding the identity of the natural person when asserting the rights of the respective data subject, you deleted the complainant's data and notified him of this fact.

In this specific case, you provided no grounds as to why you raised doubts regarding the complainant's identity.

You have modified your processes for deleting player accounts accordingly.

II.

The reprimand is based on Art. 58 (2) lit. b GDPR, as an infringement occurred against the provisions of the GDPR within your scope of responsibility.

In accordance with Art. 12 (3) sentence 1 GDPR, the controller must inform the data subject of the measures generally taken immediately following receipt of the request, and in any event within one month after receipt of such request pursuant to Art. 15-22 GDPR. The controller shall therefore provide information, confirm the erasure of data or acknowledge the objection, or at least state why this is not possible within the time period specified. Where necessary, the deadline may exceptionally be extended by a further two months in view of the complexity and number of requests. However, the GDPR does not stipulate an automatic or standard extension of the deadline without an examination of the specific case.

In this case, the complainant submitted a request to erase his personal data on January 24th, 2019. On 27th January 2019 he was then asked to provide additional information, as your company sought to ascertain that the complainant was the owner of the account. No deletion of data was carried out due to the request for further information to establish the complainant's identity.

In accordance with Art. 12 (6) GDPR, the controller may only request additional information which is necessary to confirm the identity of the data subject if reasonable doubts exist as to the identity of the natural person. Here, the principle of data minimisation must be observed pursuant to Art. (5) 1 p. 1 lit. c GDPR.

The complainant sent the request to erase his data via the support area of the account management section after logging in using his saved registration data.

The request for additional data did not represent data minimisation for identification purposes within the meaning of Art. 5 (1) p. 1 lit. c GDPR. The request for such extensive data was unnecessary, and made it more difficult for the data subject to exercise the right to erasure.

The response received on 1st October 2019 to the plaintiff's request dated 24th January 2019 to erase his data is, in our opinion, belated. This is a violation of Art. 12 (3) GDPR and Art. 12 (6) GDPR.

In view of the specific circumstances based on the facts and having concluded our investigation, we consider a reprimand is appropriate. We have established a violation on your part in the first instance. In response to our presentation of the facts, you acknowledged your actions and have stated that you will comply with the relevant data protection regulations and cease the conduct forming the subject matter of the complaint. You have modified your deletion processes accordingly.

We are confident that you will comply with the data protection regulations in future, and now consider the matter closed.

Best regards,

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

Background information

Date of final decision:	19 February 2020
LSA:	DE-Berlin
CSAs:	AT, BE, DE, ES, FR, IE, PL, PT, UK
Controller:	Sandbox Interactive GmbH
Legal Reference:	Transparency (Article 12), Right to erasure (Article 17)
Decision:	Infringement of the GDPR, Reprimand
Key words:	Right to erasure, User account, Identity

Summary of the Decision

Origin of the case

The complainant requested to have his player account deleted from the controller database of the online game he had previously bought. The controller requested additional information in order to process the erasure request, which it eventually granted nine months after the complainant's request and after being notified by the Berlin DPA.

Findings

The LSA found that the complainant requested to have his account deleted via the support function of his account, after logging in using his registration data. Although the controller may only request additional information in case of reasonable doubt regarding the identity of the natural person, the controller, in this case, did not explain why he had doubts regarding the complainant's identity. Hence, the request for additional data was not only unnecessary, but also made it more difficult for the complainant to exercise his right to erasure. Furthermore, the LSA found that not only the controller did not inform the complainant about whether they are processing the erasure request or if there is an extension of the deadline imposed by the GDPR, but also granted the erasure request with a significant delay after the end of the legal deadline.

Following the LSA's inquiry, the controller modified his process for the deletion of user accounts.

Decision

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

Summary Final Decision Art 60

Complaint

No infringement of the GDPR

Background information

Date of final decision:	2 October 2019
LSA:	DE-Brandenburg
CSAs:	AT, BE, DE-Berlin, DE-Hesse, DE-Lower Saxony, DE-Mecklenburg-Western Pomerania, DE-North Rhine-Westphalia, DE-Saarland, DE-Thuringia, DK, ES, FR, HU, IT, LU, NO, PL
Legal Reference:	Right of access (Article 15), Principles relating to processing of personal data (Article 5)
Decision:	No infringement of the GDPR
Key words:	Right of Access, Legal Age, Verification Process

Summary of the Decision

Origin of the case

The complainant requested access to his personal data processed by the controller. The controller verified the data subject's identity, and subsequently informed the complainant that his account had been suspended due to a discrepancy between the information concerning his age on his account and the information he had provided for the verification of his identity for the request. Since he was 15 years old at the time and thus a minor, he was also asked to send parental consent, a copy of his ID card and of his birth certificate, in order to access his personal data. The complainant filed a complaint to the CSA on the basis that the information he had provided for the verification process was wrongly used to suspend his account, instead of being used for the process of giving access to personal information.

Findings

The controller underlined that at the time of the request there was no standardised process in place within the company for requests by minors, since the contractual relationship between the controller and the data subjects depends on the fact that the data subjects are adults. Quickly after the controller requested additional documentation for parental consent, this request was set aside and access to

personal data was in fact given to the complainant. Finally, further measures were taken by the controller to improve the data access process.

Decision

The request for information was answered in due time and the controller's verification process has been modified in a suitable manner. The LSA therefore found that there was no infringement of the GDPR.



17 October 2019

Final Decision

Complaint against [REDACTED] – Right of access (art. 15 GDPR)

IMI Article 56 No.: 54930

IMI Case Register entry: 62334

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter “HBDI”) refers to the complaint of [REDACTED] (hereinafter “Complainant”) against [REDACTED] (hereinafter “[REDACTED]”) lodged with the Austrian Data Protection Authority.

1. Case Description

The underage Complainant requested access to and a copy of his personal data processed by [REDACTED] (Right of access - art. 15 GDPR). He submitted all information necessary for his identification by email on 25 July 2018. [REDACTED] confirmed the receipt of his email on the same day.

On 29 August 2018 the Complainant lodged a complaint with the Austrian Supervisory Authority stating that he had not yet received a reply to his request.

2. Investigation Procedure

HBDI contacted [REDACTED] in April 2019. In its immediate answer [REDACTED] stated that at the time of the Complainant's request the number of complex, data protection related customer queries had suddenly increased, making it impossible for [REDACTED] to observe the one-month time limit. The Customer Service by mistake did not send a notice to the Complainant within one month. On 5 September 2018 [REDACTED] informed the Complainant about the aforementioned difficulties and the necessary extension of the period according to art. 12(3) GDPR. According to the information provided by [REDACTED] the request finally was answered and right of access was granted by [REDACTED] on 28 September 2018, even before [REDACTED] has been contacted by HBDI. [REDACTED] stated that their internal processes had already been improved to ensure that timely responses can be given in similar cases by now.

3. Decision

[REDACTED] failed to inform the Complainant about the necessary and legitimate extension within the one-month time period set out in art. 12(3) GDPR. [REDACTED] admitted the failure, attributing this to an extraordinary number of customer queries in a period, in which GDPR had been fully applicable only for three months and a mistake in the internal processing of the request.

Considering the fact that the right to access was granted and the requested information was provided within the (extended) time limit of three months, the mere delay of a few days in informing the Complainant about the legitimate extension appears a minor infringement, which only slightly affects the Complainant's rights and freedoms.

After consideration of the significance of the infringement, [REDACTED] cooperation in the investigation process and particularly the improvement action already taken by [REDACTED] HBDI, in its draft decision dated 03 July 2019 (IMI No. A60DD 283423), considered that the investigation proceedings can be concluded and no further supervisory measures are necessary.

Within four weeks, the following supervisory authorities concerned commented on the draft decision:

The Finnish Data Protection Authority stated that it agrees with the findings of the HBDI.

The French Data Protection Authority commented on the draft decision stating that a procedure to confirm identity of the data subject where the controller would require more information than what had provided to use the service at first, would be disproportionate and not compliant with the GDPR. This comment was taken into account and HBDI can inform that [REDACTED] did not request more information than already provided.

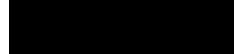
The Italian Data Protection Authority asked whether the Hessian Data Protection Authority issued a reprimand. HBDI affirmed that it had already issued a reprimand and pointed out to [REDACTED] that necessary information about requests from data subjects under art. 15-22 GDPR shall be provided without undue delay and no later than one month after receipt of the request.

The Austrian Data Protection Authority expressed an objection and asked whether HBDI had yet informed the Complainant of the outcome of the investigation and whether any statement on his part (approved by his father to the fact that the Complainant is a minor) had been taken into account. As the HBDI had not yet informed the Complainant, HBDI provided the colleagues from the Austrian Data Protection Authority in the course of an Article 61 Voluntary Mutual Assistance Procedure (IMI No. A61VM 80626) with [REDACTED] statement in order to forward it to the Complainant and

grant him his right to be heard. The Austrian Data Protection has since indicated that the Complainant has withdrawn the complaint.

As the comments made by the supervisory authorities concerned were addressed and as the Complainant apparently considers the originally alleged infringement to be eliminated, HBDI will not carry out any further supervisory measures and close the file.

On behalf of the HBDI



Summary Final Decision Art 60

Complaint

Infringement of Article 15 GDPR and reprimand

Background information

Date of final decision:

17 October 2019

LSA:

DE-Hessen

CSAs:

AT, BE, ES, DE (Berlin), DK, FI, FR, IT, NO, SK

Controller:

Nintendo of Europe GmbH

Legal Reference:

Right of access (Article 15)

Decision:

Infringement of Article 15 GDPR and reprimand

Key words:

Right of access, Data subjects' rights, Data subject access request

Summary of the Decision

Origin of the case

The complainant filed a complaint with the AT CSA contending that the controller did not comply with his access request within the one-month period, as established in Article 12(3) GDPR.

Findings

When contacted by the LSA, the controller explained that the number and the complexity of the data-related customer queries at the time of the request justified an extension of the one-month period. Additionally, by mistake, no notice of the extension had been sent to the complainant within the deadline. However, shortly after the deadline, the controller did send the complainant a notice of the extension. The access request was complied with within the extended timeframe.

Decision

The LSA found that there was an infringement of Article 15 GDPR, since the controller did not comply with the complainant's access request in the established timeframe and issued a reprimand to the controller. However, the controller had cooperated with the LSA during the investigation and notified the complainant of the justified need for an extended timeframe shortly after the due date, and answered the request within the extended timeframe. Therefore, the LSA decided not to take any further measures against the controller.

Comments

Comments received on the draft decision from the FI, FR, IT and AT CSAs were fully addressed by the LSA in the final decision. Additionally, the AT CSA indicated that the complaint was withdrawn in the course of the investigation.



Baden-Württemberg

THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 · D-70025 Stuttgart

[REDACTED]

Notification of a personal data breach

Dear [REDACTED]

Thank you very much for your notification of a personal data breach of February 15, 2019, in which you state the following:

On February 13, around 12.30pm, all employees of [REDACTED] received an e-mail from the account [REDACTED] with a PDF attachment. This was reported to IT because the text in the e-mail was in English and this employee otherwise never communicates in English. There was a fake DocuSign link in the PDF with the aim of account phishing.

In the account of [REDACTED] there was a rule activated in the inbox which deletes all incoming e-mails immediately. Therefore it is to be assumed that the account was compromised and that there is no mail spoofing.

The phishing e-mail sent also went to external e-mail addresses. In total (external and internal) approximately 850 e-mail accounts.

As possible consequence you reported that identity theft may be possible if the recipient has fallen for the phishing attachment.

You explained that as corrective actions the password of the affected account was changed immediately. All employees were informed and the danger of the e-mail was pointed out. All recipients who were read out via the Microsoft log would be informed on the day of the notification.

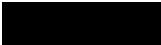
A support ticket was opened with Microsoft today to identify the attacker via IP.

You write that the personal data breach has been communicated to the data subjects and that it was recommended to delete the e-mail and, in case that the attachment has already been opened and the own account data have been entered there, to change the account password.

The notification had been submitted within 72 hours after having become aware of it and it describes the nature of the personal data breach as well as its likely consequences and the measures taken to address the data breach as required in Article 33(1) and (3) GDPR. Also, the concerned data subjects have been informed as per Article 34 GDPR.

From our point of view, the corrective measures taken by you are in order.

Unless new and relevant findings will occur in this matter, we hereby close the case.

Yours sincerely
on behalf


Summary Final Decision Art 60

Data Breach Notification

No infringement of the GDPR

Background information

Date of final decision:	27 January 2020
LSA:	DE-Baden-Wuerttemberg
CSAs:	All SAs
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No infringement of the GDPR
Key words:	Personal data breach, Phishing emails

Summary of the Decision

Origin of the case

The controller stated that a phishing attack had been launched on their central servers. The email address of a subsidiary's manager had been compromised and used to send phishing emails to employees and clients.

Findings

The LSA found that the controller had carried out an investigation and a risk assessment of the breach, before communicating it to the LSA within 72 hours of becoming aware of it, as well as to the data subjects. Further, the password of the affected account was immediately changed. They also stated that the employees had been informed about the phishing attempt.

Decision

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



Baden-Württemberg

THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 · D-70025 Stuttgart

Date 24 September, 2019

Name [REDACTED]

Ref. [REDACTED]

 Complaint of [REDACTED]
[REDACTED]

Your letter of September 04, 2019

Dear [REDACTED]

We thank you for your above mentioned letter. In this letter you have informed us that you have responded to the complainant's e-mail request for erasure of January 04, 2019, and confirmed the deletion of the personal data. We therefore consider the matter to be closed.

We want to reiterate again that the controller must comply with Article 12(3)(1) in conjunction with Article 17 of the GDPR and shall, in principle, within one month of receipt of the request for erasure, state whether they have complied or will comply with it.

We would also like to draw your attention to the fact that pursuant to Article 83(5)(b) GDPR, anyone who does not comply with the rights of the data subject as per Articles 12 to 22 of the GDPR, is acting disorderly. This administrative offence can be sanctioned with a fine of up to EUR 20,000,000, in the case of companies up to 4% of the total worldwide annual turnover of the preceding financial year, Article 83(5) GDPR.

We request you to observe this legal situation in the future.

Yours sincerely
on behalf

A solid black rectangular box used to redact a handwritten signature.

Summary Final Decision Art 60 Complaint

No infringement of the GDPR

Background information

Date of final decision:	24 September 2019
LSA:	DE -Baden-Wuerttemberg
CSAs:	All SAs
Legal Reference:	Transparency (Article 12), Right to erasure (Article 17)
Decision:	No infringement of the GDPR
Key words:	Exercise of data subjects rights, Erasure request

Summary of the Decision

Origin of the case

The complainant alleged that the controller did not comply with her erasure request.

Findings

The LSA found that the controller deleted the complainant's personal data. However, the controller did not do so within the timeframe provided by the GDPR. In its reply to the LSA, the controller described the measures taken to avoid delays in the future.

Decision

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

Berlin Commissioner for Data Protection and Freedom of Information

Final decision concerning the data breach reported by Foodora GmbH / Delivery Hero SE

We will close the case about the data breach reported by Foodora GmbH / Delivery Hero SE. According to our recommendations, the company has informed the 30 affected data subjects (seven from Germany, four from France, four from Italy, seven from Sweden, four from Norway, one from Finland, three from Austria) according to Art. 34 GDPR. The information was provided in the respective national language.

We believe that the controller has taken adequate technical and organizational measures. Thus the faulty function was immediately switched off until the correction (the download function of the personal data was completely deactivated), later the functionality of the data export was again activated, with regard to the details we refer to the answer of the company about the countermeasures.

Consideration was also given to the fact that the data only reached a single data recipient, who reported the error himself and was requested to delete the data.

Summary Final Decision Art 60

Complaint

Reprimand to controller

Background information

Date of final decision:	31 October 2018
LSA:	DE- Berlin
CSAs:	AT, BE, DK, LU, SE, DE- Bavaria, DE-Hesse, DE-Lower Saxony, DE-Mecklenburg-Western Pomerania , DE-Saarland
Controller:	Outfittery GmbH
Legal Reference:	Right to erasure (Article 17), Right to object (Article 21)
Decision:	Reprimand to controller
Key words:	Lawfulness of the processing, Rights of data subjects, Right to erasure, advertising

Summary of the Decision

Origin of the case

The complainant sent an e-mail to the controller requesting that he no longer receives any further emails, in particular advertising e-mails, and that he requests access to and erasure of his personal data. The complainant subsequently received further advertising e-mails. Information on the personal data processed and the notice of erasure were sent to the complainant.

Findings

The LSA considered that the controller had violated art. 17(1)(c) in conjunction with art. 21(2) GDPR because according to it the data subject has the right to require the data controller to erase his personal data as well as to object to its processing for advertising purposes. The controller must comply with such a request immediately. However, the controller did not comply with the request until much later.

Decision

The LSA decided to reprimand the controller.

Summary Final Decision Art 60

Complaint

Reprimand to controller

Background information

Date of final decision:	3 December 2018
LSA:	DE - Berlin
CSAs:	BE, DE-Mecklenburg-Western Pomerania
Controller:	Chal-Tec GmbH
Legal Reference:	Right to erasure (Article 17), Lawfulness of processing (Article 6), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)
Decision:	Reprimand
Key words:	Right to erasure, exercise of the rights of the data subject, lawfulness of the processing, e-Commerce

Summary of the Decision

Origin of the case

The complainant created an account on the controller's website, and the same day he asked for its deletion. Despite receiving a confirmation e-mail about the deletion, the complainant could still log in to his account. In an e-mail, the data controller told the complainant that for legal reasons the account could not be deleted, but only deactivated.

Findings

Following a request for information by the LSA, the data controller deleted the account. The improper handling of the data subject's request was due to keeping two separate databases, each handled by a different department of the controller which had miscommunicated in this case.

Decision

The LSA decided to reprimand the data controller as the removal of the complainant's personal data was not carried out by the time it was due, i.e. per art. 58(2)(b) GDPR.

Comments

Even though the request was submitted by the complainant prior to the entry into force of the GDPR, on 25 May 2018 the account had not been deleted yet and therefore, the LSA states that the GDPR is applicable.

BInBDI

- () Entwurf gefertigt (von/am) _____ Vor Abgang z.K. () Chefin _____ () AbtL _____
() Reinschrift (von/am) _____ Nach Abgang z.K. () Chefin _____ () AbtL _____
() anonymisiert in Grundsatzvorgang abzulegen
() Durchschrift senden an
() behördlichen / betrieblichen Datenschutzbeauftragten entworfen (von/am) _____ schlussgezeichnet von _____
() _____
() _____ abgeschickt (von/am) _____
() Anlage(n)

Chal-Tec GmbH
Wallstraße 16
10179 Berlin

Geschäftszeichen:
(bitte angeben) 521.9685.10
Abteilung: I B
Bearbeiter(in):
Telefon:
Durchwahl-Nr.:
[REDACTED]

Datum: December 3rd, 2018

Reprimand

Your letter of August 15th, 2018

To whom it may concern,

we hereby reprimand your company for a violation of the General Data Protection Regulation (GDPR) in the processing of personal data in your area of responsibility.

Explanatory memorandum:

Our decision is based on the following considerations:

I.

We have established the following facts: On March 24th, 2018, the complainant opened an account on the electronic star website, which is operated by your company. He placed an order which he canceled on the same day. Along with the cancellation, he asked for his account to be deleted. The cancellation and the deactivation of his account were confirmed immediately. Since the complainant could still log in to his account after the confirmation, he asked, why his account had not been deactivated against the assertion of your employees. In an e-mail on the 27th of March your customer care explained that for legal reasons they were not able to delete the account, but could deactivate it.

You responded to our request for information from the 10th of July 2018, by informing us, that it was a mistake. The account of the complainant was now permanently deleted, but only after our request for information had reached you. Before that, the complainant's request was not handled. This is due to the fact, that you keep two separate data bases: A customer data base, which your customer care

administers, and a customer user data base, which your in-house shop management administers. The customer care took all necessary steps to deactivate the profile in the customer data base, but they did not forward the request to the shop management. You therefore stated, the reply to the complainant was unclear and by now obsolete.

II.

The reprimand is based on Article 58 paragraph 2 letter b of the GDPR. There was a violation of the GDPR in your area of responsibility, since you deleted the complainant's account with a delay. The GDPR is applicable, as the account was not deleted by the 25th of May, 2018.

Personal data is to be deleted according to Article 17 paragraph 1 letter a, b, and c of the GDPR, if it is no longer necessary for the data controllers' purposes that it was retrieved for, the consent is withdrawn and there are no overriding legitimate grounds for the processing. With the request for erasure, the complainant expressed, that he is not interested in maintaining an account. Therefore his data is no longer necessary to maintain a contract relationship. At the same time, his request is to be viewed as a withdrawal of his consent. There are no overriding legitimate ground for processing his data, as the complainant canceled his order in an early stage, so his information is not necessary for tax reasons.

The deletion should be carried out within a month after receiving the request, about which the complainant is to be informed, Article 12 paragraph 3 sentence 1 in connection with 17 GDPR. The complainant requested the deletion of his account on the 24th of March, but it was only executed on the 10th of July. As data controller, you have to make sure that the rights of the people concerned are effectively implemented. This means you must make sure that you take all necessary technical and organizational measures as well as sufficiently informing your employees.

Taking the specific circumstances of the facts determined into account, we consider a reprimand to be appropriate after the completion of our investigation. We have found a violation on your part for the first time. As a reaction to our hearing, you showed understanding and announced that you would comply with GDPR and put an end to the reprimanded conduct. You now deleted the complainant's account.

Note: If you disregard this reprimand or continue to violate the GDPR, we will consider additional measures, such as imposing a data processing restriction, including a ban, or a fine on you. We are also authorized to bring infringements of the GDPR to the attention of the judicial authorities and, if necessary, to initiate legal proceedings in order to enforce the provisions of the GDPR.

This reprimand has been coordinated with the supervisory authorities of Belgium and Mecklenburg-Western Pomerania.

With kind regards

631.30 and 535.461

Berlin Commissioner for Data Protection and Freedom of Information

Final decision concerning the data breach reported by AWIN AG

Ladies and gentleman,

As you know, our authority, as lead supervisory authority, has informed the concerned supervisory authorities in Europe about the above mentioned notification and the measures (Art. 60 GDPR) because of the cross-border nature of the processing.

The case has been closed.

Justification:

According to our recommendations, the controller has taken precautionary measures and on 8 February 2019 placed a notification pursuant to Art. 34 (3) (c) GDPR on their German and British websites. The notifications remained online at least until the end of March 2019 and are available at

<https://www.awin.com/de/dsgvo/mitteilung> and

<https://www.awin.com/gb/gdpr/notifications>.

Of the 47 stolen laptops, only nine had unencrypted hard disks (see e-mail from the controller of 5 November 2018). In due consideration of Art. 34 (3) (a) GDPR, we concentrated on these nine laptops in the further processing.

In order to find out whether and if so which personal data of business clients were stored on the laptops and if there is an obligation to notify the data subject according to Art. 34 GDPR the controller determined to which (former) employees the laptops were assigned to. From the computer codes starting with MUC, PAR and LON it, 7 laptops could be assigned to the Munich branch, one to the Paris and one to the London branch. Accordingly it was assumed that there are concerned data subjects in France, the UK and Germany.

As both working students and junior employees do not process any personal data on their laptops, and out of the seven German laptops four were assigned to working students and a junior employee, our focus remained on three laptops in Germany and one in the UK.

Against this background the notification was put online by the controller in German and in English.

With regard to France the controller confirmed with e-mail dated 13 February 2019 that also the French laptop was assigned to a junior employee and did therefore not process any personal data. Therefore the planned notification in French remained unpublished.

Summary Final Decision Art 60

Data Breach Notification

No violation

Background information

Date of final decision:	3 April 2019
LSA:	DE-Berlin
CSAs:	DE-Lower Saxony, UK
Controller:	AWIN AG
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:	No violation
Key words:	Data breach

Summary of the Decision

Origin of the case

The controller reported a data breach to the LSA after some laptops were stolen. The laptops contained personal data of business partners, but the majority of the laptops had encrypted hard disks.

Findings

Only 4 laptops could have included personal data, 3 of which were located in Germany and one in the UK. The controller posted breach notifications online following the recommendations by the LSA as per Article 34(3)(c) GDPR.

Decision

The case was closed as the controller followed the recommendations of the LSA.



Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin

Billpay GmbH
Geschäftsführung
Zinnowitzer Straße 1
10115 Berlin

Geschäftszeichen:
(bitte angeben) 521.10197.7
Abteilung: [REDACTED]
Bearbeiter(in): [REDACTED]
Telefon: [REDACTED]
Durchwahl-Nr.: [REDACTED]

Datum: 2. Juli 2019

Verwarnung

Beschwerdeführer:

Ihr Schreiben vom 26. November 2018

Sehr geehrte Damen und Herren,

hiermit verwarnen wir Ihr Unternehmen wegen eines Verstoßes gegen die Datenschutz-Grundverordnung bei der Verarbeitung personenbezogener Daten in Ihrem Verantwortungsbereich.

Begründung:

Unserer Entscheidung liegen die nachstehenden Erwägungen zugrunde:

I.

Wir haben folgenden Sachverhalt festgestellt:

Der o. g. Beschwerdeführer hat sich am 25. Mai 2018 per E-Mail unter Angabe seiner aktuellen Anschrift an die Billpay GmbH mit der Bitte um Auskunft über seine von Ihnen verarbeiteten personenbezogenen Daten gemäß Art. 15 Datenschutz-Grundverordnung (DS-GVO) gewandt. Mit Schreiben vom 28. Mai 2018 haben Sie versucht, dem Beschwerdeführer die gewünschte Auskunft per Einschreiben zu erteilen. Dieses konnte jedoch dem Beschwerdeführer nicht zugestellt werden, da Sie eine andere als die im Auskunftsersuchen des Beschwerdeführers angegebene postalische Adresse verwendet haben. Mit E-Mail vom 4. Juli 2018 haben Sie den Beschwerdeführer um Mitteilung seiner aktuellen Anschrift gebeten und vorgetragen, diese E-Mail sei seitens des Beschwerdeführers unbeantwortet geblieben.

Eine Auskunft über seine personenbezogenen Daten haben Sie dem Beschwerdeführer am 26. Oktober 2018 erteilt.

II.

Die Verwarnung beruht auf Art. 58 Abs. 2 lit. b DS-GVO. Es kam zu einem Verstoß gegen die DS-GVO in Ihrem Verantwortungsbereich.

Die Billpay GmbH hat gegen Artikel 12 Abs. 3 DS-GVO verstoßen. Nach Art. 12 Abs. 3 Satz 1 DS-GVO muss der Verantwortliche der betroffenen Person auf Antrag unverzüglich Auskunft erteilen, spätestens aber innerhalb eines Monats.

Nach Art. 24 Abs. 1 DS-GVO sind seitens des Verantwortlichen geeignete technische und organisatorische Maßnahmen zu treffen, um die Einhaltung dieser Frist sicherzustellen. Eine Adressierung der Auskunft an die vom Beschwerdeführer in seinem Auskunftsersuchen angegebene Anschrift wäre für die Billpay GmbH technisch möglich und auch zumutbar gewesen.

Mithin erfolgte die Beantwortung des Auskunftsersuchens des Beschwerdeführers vom 25. Mai 2018 am 26. Oktober 2018 verspätet. Es liegt damit ein Verstoß gegen Art. 12 Abs. 3 DS-GVO vor.

Unter Berücksichtigung der konkreten Umstände des ermittelten Sachverhalts halten wir nach Abschluss unserer Untersuchung eine Verwarnung für angemessen. Wir haben erstmalig einen Verstoß Ihrerseits festgestellt. Auf unsere Ansprache hin zeigten Sie sich einsichtig und kündigten an, datenschutzrechtliche Vorgaben einzuhalten und das gerügte Verhalten abzustellen.

In sicherer Erwartung, dass Sie sich zukünftig an die datenschutzrechtlichen Vorschriften halten werden, betrachten wir die Angelegenheit als abgeschlossen

Mit freundlichen Grüßen

[REDACTED]

Summary Final Decision Art 60

Complaint

Reprimand to controller

Background information

Date of final decision:	2 July 2019
LSA:	DE-Berlin
CSAs:	AT, DE-Rhineland-Palatinate, DE-Hesse, DE-Saarland, DE-North Rhine-Westphalia, FR
Controller:	Billpay GmbH
Legal Reference:	Right of access (Article 15), Responsibility of the controller (Article 24), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)
Decision:	Reprimand to controller
Key words:	Right of access, Exercise of the rights of the data subjects, Reprimand, Data Subject Rights not respected

Summary of the Decision

Origin of the case

The complainant sent an e-mail to the controller, stating his current address, requesting access to his personal data in accordance with Article 15 GDPR. The controller attempted to provide the complainant with the requested information by a registered letter, but it used another postal address than the one specified by the complainant. Therefore, the letter was not delivered to the complainant. The controller sent an e-mail to the complainant requesting his current address. As a result, the complainant was provided with the information about his personal data four months after the deadline established under Article 12 (3) GDPR.

Findings

The LSA determined that the controller infringed Article 12(3) GDPR by exceeding the deadline to answer the complainant's access request, since it was technically possible and reasonable for the controller to send the information to the address given by the complainant, without further delay.

Decision

Taking into account the circumstances of the case and the fact that the controller, after being contacted by the LSA, showed understanding and its willingness to comply with data protection regulations, the LSA issued a reprimand based on Article 58(2)(b) GDPR for violating the complainant's right of access under Article 15 GDPR.

OUTFITTERY GmbH
Leuschnerdamm 31
10999 Berlin

Reprimand
Your letter of 27 September 2018

Ladies and Gentlemen,

We hereby reprimand your company for a violation of the GDPR with regard to the processing of personal data in your responsibility.

Reasons:

Our decision is based on the following considerations:

I.

We have established the following facts:

On 3 July 2018 (at 15:06), the complainant sent an e-mail to OUTFITTERY GmbH, addressed to service@outfittery.de, requesting that OUTFITTERY GmbH no longer sends him any further e-mails, in particular advertising e-mails, and that he requests access to and erasure of his personal data. The complainant received further advertising e-mails from OUTFITTERY GmbH on 19 July 2018 and 3 August 2018. Information on the personal data processed and the notice of erasure were sent to the complainant on 28 August 2018.

II.

The reprimand is based on Article 58(2)(b) of the GDPR. There has been a violation of the GDPR in your responsibility.

Under Article 17(1)(c) 2nd Alternative GDPR, the data subject has the right to require the controller to erase personal data relating to him or her without delay. The data controller is also obliged to erase the personal data immediately if the data subject has objected to the processing of his/her personal data for advertising purposes pursuant to Article 21 (2) GDPR.

By his request on 3 July 2018, the complainant stated that he was not interested in further advertising information from OUTFITTERY GmbH. Consequently its behavior is to be understood as advertising objection in the meaning of the art. 21 Abs. 2 GDPR. Such an advertising objection leads to a deletion obligation according to Article 17 (1)(c) 2nd alternative GDPR. The timeframe to be applied here is "immediately".

However, a deletion from the distribution list did not take place. OUTFITTERY GmbH did not fulfil its obligation to delete the e-mail address for advertising purposes until 28 August 2018 and sent further advertising e-mails to the complainant on 19 July 2018 and 3 August 2018.

If the data subject exercises the right to object in the case of direct marketing in accordance with Art. 21 (2), further processing is automatically and unconditionally unlawful in accordance with Art. 21 (3) GDPR when the objection is raised.

According to article 12 (3) GDPR the controller has to provide the information required according to article 15 and/or article 17 GDPR usually immediately, in each case within one month after

receipt of the application. This period may exceptionally be extended by a further two months if this is necessary taking into account the complexity and number of requests. However, a standard and general extension of the period without examination of the individual case is not intended by the GDPR. OUTFITTERY GmbH did not comply with its obligation to give access to the personal data concerning the complainant in due time and did not provide this information before 28 August 2018.

Taking into account the specific circumstances of the case, we consider a reprimand to be appropriate after completion of our investigation. For the first time, we have identified a violation of the GDPR by the controller. Upon our intervention, you showed understanding and announced that you would comply with data protection regulations and stop the reprimanded conduct.

Yours sincerely

[REDACTED]

[REDACTED]

[REDACTED]

Legal Department

by IMI

Date : 2nd October 2019
Contact: [REDACTED]
Tel: [REDACTED]
Fax: [REDACTED]
National Reference: [REDACTED]

Final Decision – Complaint against [REDACTED]

- IMI A56ID 55264
- IMI Case Register entry 58950
- IMI A60DD 74979

Dear colleagues,

on 27 August 2019, the above-mentioned draft decision was submitted to the supervisory authorities that have reported to be concerned. Within the four-week period, no relevant and reasoned objection was expressed. Therefore the complaint will now be closed without further actions on the basis of the draft decision cited below. For this purpose, a closing message was sent to the controller today, which contained the relevant extracts from the draft decision. The controller was also informed of the note made by the French CNIL on 23rd September 2019 under "Other relevant comments".

I. Submission of the complaint; competence

On 31st August 2018, the then 15-year-old complainant filed a complaint against [REDACTED] with the Austrian data protection authority ("ÖDSB") regarding the [REDACTED] roof of parental consent to raise the complaint at issue was submitted to the ÖDSB.

[REDACTED] is the contractual partner and controller for all (registered) users [REDACTED] on the following websites: [REDACTED] With regard to these websites, [REDACTED] maintains its (main) establishment within Europe in [REDACTED] [REDACTED]. The website [REDACTED] is operated by [REDACTED] which is therefore not subject to this draft decision.

The signature of customer service messages, as received by the complainant, mentions [REDACTED] [REDACTED] owever, this company only provides services on behalf of [REDACTED] as a processor. The [REDACTED], which is also located in [REDACTED], is therefore not controller with regard to the subject of the complaint to be assessed below. We have already pointed out to [REDACTED] that the signature of the customer service messages should reflect the relationship more clearly.

[REDACTED]

Since the case could constitute cross-border processing under Art. 4 No. 23 lit. b GDPR, the ÖDSB initiated an Art. 56 identification procedure (A56ID 63640) in IMI in December 2018 for further clarification. Due to the controller's main establishment in [REDACTED]

[REDACTED] is according to art. 56 GDPR and § 19 Federal Data Protection Act the lead supervisory authority for cross-border processing activities of the controllers. The [REDACTED] confirmed its competence to investigate the case via IMI on 7th January 2019 and created the case register entry no. 58950 on 29th January 2019.

II. Facts of the case

The complaint documents containing the conversation between the complainant and the [REDACTED] customer service show that the complainant requested information about his user account [REDACTED] on 1 July 2018 via a contact form (please see the complaint attachments uploaded under "relevant documents"). On 5th July 2018 [REDACTED] customer service responded via e-mail by asking the complainant to verify his identity in order to ensure that the information was provided only to the data subject.

It is known to the [REDACTED] from previous supervisory activities that data access requests can be submitted to the controller by e-mail, contact form or post; there is not (yet) any possibility of submitting a request from the user account whilst logged in. [REDACTED] in general provides different modes of identity verification (including telephone verification). In cases where data access of a certain volume is requested, the user – for different reasons already detailed to us in a previous case – is first asked to provide verification by means of a redacted copy of his or her ID – as was the case with the complainant. In such requests for proof of identity it is expressly pointed out to the user that various specific data fields may be redacted. According to the current process implemented by the controller since November 2018, all fields may be redacted except name, date of birth, period of validity and address (at the time of the complainant's request, it had not yet been explicitly stated that photo, title, signature and ID number can also be redacted). Name, address and date of birth are data categories which [REDACTED] asks its newly registered website users to provide before the [REDACTED] and which are verified in the course of the contractual relationship (depending on the type of user account, [REDACTED] etc.) by different methods (e.g. [REDACTED]). For the submission of the redacted copy of the identity document, various options are explained to the applicants and (since November 2018) indications are given as to the degree of security of the respective option.

The aforementioned e-mail of 5th July 2018 also indicated that the proof of identity and address "will be used exclusively for the purpose of identity verification in connection with the requested data access".

The complainant then passed the requested verification process and received feedback from [REDACTED] customer service on 1st August 2018, stating that his user account had been suspended as there were indications that the complainant had not yet reached the age of majority. For this reason, the message stated, the company's general terms and conditions did not allow the complainant [REDACTED] According to [REDACTED] T&C (as of May 2018) [REDACTED]

On 2nd August 2018, the [REDACTED] customer service also informed the complainant (translated by [REDACTED])

"Unfortunately we cannot give you the data as things stand because you are not yet of age. We need your parents' consent, as well as the birth certificate and a copy of your parents' identity card."

On 3rd August 2018, the complainant replied (translated by [REDACTED])

"I don't think you've been properly informed. According to the (Austrian) Data Protection Code, the processing of my data with my consent is legally binding with the completion of age 14. Therefore I may make dispositions with regard to my data and I urge you to grant me my right to information. Otherwise, I will seek to complain to the competent authority."

In the original complaint submitted to the ÖDSB, the complainant described the following in response to the question as to how the controller had reacted to his request for information (translated by [REDACTED])

"I was told that my account had been deactivated because it turned out during the processing of my request that I was under the age of majority.

I consider this answer to be inadequate and believe that my rights have been infringed for the following reasons.

My account has been deactivated although I have only requested information. I have never intentionally given false information about my birth date. The fact that I made a request for information was used against me, which is certainly not appropriate."

The case description of the ÖDSB in the A56 identification procedure contains the following summary:

"On 1 July 2018, the complainant sent a request demanding access for information by a contact form to the controller. The controller replied to the complainant that he could not easily provide information because the complainant was not of legal age and therefore had to provide the controller with the consent of his parents, his birth certificate and a copy of his parents' identity card."

Following an initial oral request for comment to the company's data protection officer on 15th January 2019, the [REDACTED] was informed that [REDACTED] does not provide standardized processes for requests from minors, as such requests could not normally occur because minors are not allowed to register for the service. The customer services demand for further documents was therefore not a requirement of the company and, from its point of view, under no aspect necessary.

By letters dated 25th February and 7th March 2019, which have been brought to the ÖDSBs attention, the [REDACTED] turned to the German-speaking complainant directly in order to ask further questions about the subject matter of the complaint. The background is that, from the [REDACTED] perspective, the complaint is not directed against the fact that a birth certificate and copies of the parents' identity cards were requested, but against the fact that information from the copy of the identity card was used for comparison with the data stored in the user account and that the user account was suspended due to the discrepancy found.

On 28th February and 16th March 2019, the complainant informed the [REDACTED] that this was the case (translated by [REDACTED])

"You have correctly recognized that my complaint is directed against the suspension of my user account. It is also clear to me that this is not a data protection matter, which is why this fact is of secondary importance.

I see the data protection problem in the fact that my personal data (the copy of my passport) have been used contrary to the original purpose. I also disagree with your statement that I "did not provide the company with the copy of the identity document merely for the purpose of enabling the information to be transmitted". The above was, in fact, the only reason I submitted the copy of the identity card. [...]."

I have continued to communicate with the controller since 3rd August 2018. You will find my letter attached. In the meantime, I have also received the requested information, [...]."

Following a request dated 15th April 2019, [REDACTED] took the opportunity to submit its written comments by letter dated 23rd April 2019 (translated by [REDACTED])

"Our customer service received [REDACTED]'s request for information on 01.07.2018 and requested on 05.07.2018 - according to our standard process - a redacted copy of his identity card. [REDACTED] sent a copy of his passport on the same day. As it turned out that [REDACTED] was a minor and therefore had violated the [REDACTED] Terms and Conditions, his [REDACTED] user account was suspended.

We have not corrected the date of birth in the user account. Only an internal note with the correct date of birth was stored.

After [REDACTED] asked on 31.07.2018 about the status of his application, our customer service requested on 02.08.2018 (unfortunately erroneously) the consent of his parents, as well as copies of the birth certificate and the identity card of the parents in order to be able to give the data information.

After [REDACTED] complained about this on 03.08.2018, our customer service became aware of this mistake and gave [REDACTED] the desired information electronically on 16.08.2018. We have not received any further communication from [REDACTED] since then, so we consider his request to be closed."

Five internal documents, regulating the processes according to which the [REDACTED] customer service is meant to handle access requests, were then made available to the [REDACTED] by [REDACTED] on 17th May 2019:

- (1) Standard procedure for requests for data information (SARs SOP DE 2019),
- (2) Subject Access Request Standard (Global 2019),
- (3) Subject Access Redaction Guidelines (Global 2018),
- (4) Subject Access Exemption Guidelines (Global 2017),
- (5) Contact Verification (CV) for telephone/e-mail ([REDACTED]).

Document (1), in which the processes are described in the most detailed way, contains the note: [REDACTED] (this privacy team is based in [REDACTED] for German cases and at a service company in [REDACTED] for other languages). The list of documents that may be requested from the [REDACTED] customer service in

addition to or instead of a copy of an identity document only includes powers of attorney of legal representatives, certificates of inheritance in the event of death or

[REDACTED] Birth certificates or identity cards of custodians are not mentioned at any point. The above-mentioned documents also show the process by which the copies of identity cards are immediately deleted or destroyed after access to information has been granted (the [REDACTED] was able to convince itself of the practical implementation of these requirements on the occasion of an on-site meeting). Upon request [REDACTED] furthermore informed us that an applicant will be contacted by telephone (provided a valid number is stored) or in writing if a discrepancy between the data on the ID copy and the data in the user account is found. If a discrepancy cannot be resolved and doubts cannot be dispelled, access will not be provided.

III. Legal assessment

The [REDACTED] as no concerns that the verification process in its current form and as specified by the controller for customer service is compatible with the requirements and limits of Art. 12, 15 GDPR.

Before granting access to his information, the complainant initially was asked to verify his own identity, which he did immediately, without expressing any concerns about the concrete procedure. The complainant was expressly informed as to which data fields of the identity document he could black out before transmission - whether he made use of this is not known. This is, however, of no relevance for the assessment of the complaint case, since the complainant objects to the processing of his date of birth, which should remain visible in any case. The data that was not to be redacted according to the current data access process (name, date of birth, address) is data that [REDACTED] requests from its newly registered website users as a matter of course, and that it verifies with the help of external sources in the course of the contractual relationship. With regard to this data, the company therefore has a database of valid user data to compare to, which means that the verification process carried out is suitable for ensuring that the account holder and the applicant are identical and that the documents containing the information requested are only transmitted to an authorized person. Only the period of validity of the identity card is a new date for the company, the consultation of which is also necessary and suitable to ensure the aforementioned purpose.

The verification process, which was carried out differently in some details at the time of the complainant's request, has already been modified by [REDACTED] in November 2018 in order to minimize the process to the most necessary data and to make it technically and organizationally more secure.

a. Request for additional documents - Art. 12, 15 DS-GVO

In contrast to the aforementioned verification process, the [REDACTED] does not see on what legal basis an underage applicant, whose identity has already been determined, could be asked to furnish additional documents relating to the custodian before information pursuant to Art. 15 GDPR is provided. This query would not be covered by Art. 12 para. 6 GDPR, which allows the controller to request additional information necessary to confirm the identity of the data subject in cases of reasonable doubt as to the identity of the applicant. On the one hand a birth certificate or a copy of a parent's identity card has no influence on whether or not the applicant is the same as the account holder whose data is supposed to be submitted. On the other hand, in the context of the data access request, there is also no consent required of the custo-

dians. It is therefore not apparent that any documents of the custodians fulfil a purpose which justifies their request by the controller.

In the [REDACTED] s opinion this question can ultimately remain unanswered in the specific case. [REDACTED] has provided meaningful documentation to show that the customer service's request to transfer additional documents of the custodians did not comply with the controllers specifications and instructions. Rather, this was a case of faulty communication by a customer service employee in a single case. There is no reason for the [REDACTED] to doubt the information provided by the controller, especially since the [REDACTED] customer service immediately revised its initial statement following a brief note from the complainant. The requested information then was provided without any further intermediate steps. Even if one were to assume that for a short period of time an obstacle for a data subject to assert his rights had been created, it should be borne in mind that according to his e-mail of 3rd August 2018 the complainant was very familiar with his rights. At no time did he seem to be under the impression that he had to comply with the request. There was therefore only a hypothetical risk that further data would be transmitted involuntarily and without necessity in order to obtain data access.

The [REDACTED] sees no evidence of a risk of repetition in the sense that obstacles will be wrongly imposed on other minor applicants before granting data access. The controller has submitted various internal documents that comprehensively set out the internal requirements for customer service with regard to data access requests. These documents do not contain any instructions that might give cause for concern.

b. Correction of birthdate/ storage of an internal note - Art. 5, 6 GDPR

Overall the complainant's concerns are solely directed against the individual processing of his birthdate from his ID. The complainant regards this as a data processing for an unlawful purpose and thus a violation of Art. 6 para. 1 and para. 4 GDPR.

These concerns are not shared by the [REDACTED]. The [REDACTED] deems the described process as – at least – covered by Art. 6 para. 1 lit. f, para. 4 and Art. 5 para. 1 lit. d GDPR. The controller has requested data from the complainant for an identity verification and compared it with his own database. The complainant had previously been informed that his copy of the identity document would be used for the purpose of identity verification in connection with the data information provided. Against this background, the complainant did not simply make the document available in order to enable the information to be transmitted. This would be the case if someone was asked to provide the address on the ID so that it could be used [REDACTED]. Rather, the present case concerned the verification of identity, which presupposes the comparison and check of identity card and user account data in order to determine that the person submitting the application is identical to the account holder.

In the complaint case, it became apparent that there was a discrepancy between the date of birth as it appeared on the ID card and as given by the complainant himself when registering on the [REDACTED]. Even though the complainant has stated that he never intentionally provided false information, false information concerning the date of birth had been deposited in his user account for reasons which at this point cannot be ascertained anymore.

According to its own security standards, in consequence [REDACTED] should not have been able to grant data access to the complainant because it could not be determined with certainty that the applicant and the account holder matched up and because there was a risk of unauthorized

data transfer to third parties. In order to try to fulfil the complainant's interest and because in the specific case no further anomalies were identifiable with regard to the complainant's user account, the [REDACTED] customer service nevertheless completed the verification solely by means of name and address matching.

According to Art. 5 para. 1 lit. d GDPR, "personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they were processed, are erased or rectified without delay ("accuracy")". In view of this principle, after permissible data matching, a controller may not simply ignore the finding that one of the customer's data sets must be incorrect. Otherwise the controller would even risk violating Art. 6 para. 1 lit. b and Art. 5 para. 1 lit. d GDPR. In addition, the date of birth is information which has direct influence on the contractual relationship as the company according to its T&Cs expressly excludes minors from

[REDACTED] In the present case circumstances made it obvious that the birthdate in the ID had to be the accurate date. In order not to avoid violation of the accuracy requirement of the GDPR and to enforce the controller's own T&Cs, the actual birthday from the ID as well as the information that it does not coincide with the date indicated at the time of registration has been stored by [REDACTED], together with the consequence of the account suspension. Instead of immediately rectifying the data stored in the user account, only an internal note was created to alert the complainant to the suspicion and give him the opportunity to clarify.

Finally, the complainant's request for information of 1st July 2018 was also answered in due time within the meaning of Art. 12 para. 3 GDPR. In the absence of any indication to the contrary, it can be assumed that the information was provided in a satisfactory manner.

IV. Decision

Based on the foregoing facts of the case and legal assessment, the [REDACTED] considers the investigation procedure to be completed. In summary, no ongoing violation of the provisions of the General Data Protection Regulation could be found. As the complaint has only limited personal impact and due to the measures already taken by [REDACTED] to improve the data access process, the [REDACTED] does not regard as necessary any further action according to Art. 58 para. 2 GDPR. Therefore, the cross-border complaint is hereby closed.

On behalf of the [REDACTED]

[REDACTED]



12 September 2019

Final Decision

Complaint against [REDACTED] – Right of access (art. 15 GDPR)

IMI Article 56 No.: 48365

IMI Case Register entry: 63908

The Hessian Commissioner for Data Protection and Freedom of Information (hereinafter “HBDI”) refers to the complaint of [REDACTED] (hereinafter “Complainant”) against [REDACTED] (hereinafter [REDACTED]) lodged with the Cypriot Data Protection Authority.

1. Case Description

On 26 June 2018, the Complainant requested access to and a copy of his personal data processed by [REDACTED] (Right of access - art. 15 GDPR) via email. According to the Complainant’s allegations, he did not receive a response within the one-month time period set out in art. 12(3) GDPR.

2. Investigation Procedure

HBDI contacted [REDACTED] in April 2019. In its answer [REDACTED] stated that at the time of the Complainant’s request, the number of complex, data protection related customer queries had suddenly increased, resulting in a delay of about two weeks in the processing of all incoming requests.

[REDACTED] stated that on 3 August 2018, the Complainant’s request had been answered for the first time. The Complainant confirmed receipt of this letter on 8 September 2018 but he was not satisfied with [REDACTED] response since he had only received information about his personal data processed in 2018. The Complainant demanded further information about the years 2009 to 2017. [REDACTED] stated that the requested information was sent to the Complainant on 26 September 2018. Upon request, the HBDI received a copy of this letter. But it seems as if the Complainant did not receive this letter. The HBDI could not find out why this letter did not reach the Complainant.

[REDACTED] took the complaint and the HBDI’s intervention as an opportunity to provide the requested information once again to the Complainant via email on 26 April 2019. This time, the Complainant confirmed receipt of the information and was satisfied

with the response. He replied: “*Dear [REDACTED] thank you very much for sending this updated information (...)*”.

[REDACTED] stated that their internal processes had already been improved to ensure that timely responses can be given in similar cases by now.

3. Decision

[REDACTED] failed to inform the Complainant about the necessary and legitimate extension within the one-month time period set out in art. 12(3) GDPR. [REDACTED] admitted the failure, attributing this to an extraordinary number of customer queries in a period, in which the GDPR had been fully applicable only for one month.

Considering the fact that, in the meantime, the right of access was granted and it cannot be found out why [REDACTED] second letter with the requested information did not reach the Complainant, the mere delay appears a minor infringement, which only slightly affects the Complainant’s rights and freedoms.

After consideration of the significance of the infringement, [REDACTED] cooperation in the investigation process and particularly the improvement actions already taken by [REDACTED] HBDI, in its draft decision dated 04 July 2019 (IMI No. A60DD 71099),

[REDACTED] t the investigation proceedings can be concluded and no further supervisory measures are necessary. Within four weeks, none of the other SAs concerned expressed a relevant and reasoned objection to this draft decision. Therefore, on 04 September 2019, HBDI sent a concluding letter to the controller and closed the case.

On behalf of the HBDI

[REDACTED]

Summary Final Decision Art 60 Complaint

No infringement of the GDPR

Background information

Date of final decision:	12 September 2019
LSA:	DE-Hessen
CSAs:	CY, DK, ES, FR, SE
Legal Reference:	Right of Access (Article 15), Exercise of Data Subject Rights (Article 12)
Decision:	No infringement of the GDPR
Key words:	Right of access, Exercise of data subject rights

Summary of the Decision

Origin of the case

The complainant alleged that he did not receive a response to his request to access a copy of his personal data, processed by the controller, within the one-month timeframe set by the GDPR.

Findings

The LSA found that at the time of the complaint, the controller was faced with an important amount of data protection related queries, justifying the need for an extension of the timeframe. In a first reply to the request, the controller gave access only to a part of the personal data requested. The complainant reiterated the request for the remaining personal data. A second reply was sent to the complainant, which the complainant never received. Once the complaint was made to the LSA, the controller sent the letter again, which the complainant received this time. The controller also improved their internal processes for future responses to such requests.

Decision

No infringement of the GDPR was found, since appropriate action had been undertaken by the controller.

Summary Final Decision Art 60

Complaint

No violation

Background information

Date of final decision:	21 December 2018
LSA:	DE - North Rhine-Westphalia
CSAs:	DE - Rhineland-Palatinate, DE - Mecklenburg-Western Pomerania, DE - Bavaria (priv), DE - Lower Saxony, DE - Saarland, ES
Legal Reference:	Lawfulness of the processing (Article 6)
Decision:	No violation
Key words:	Direct Marketing, Legitimate interest, publicly available data

Summary of the Decision

Origin of the case

Complainant states they received postal advertisement and tried to exercise their right of access and right to erasure. The contacted branch stated that the letter was not sent to the correct recipient, as they do not manage personal data. The correct establishment is in Germany. The complainant contacted their local SA as they deem that the controller is wrongfully processing their personal data, which is stored in a publicly accessible register.

Findings

According to recital 47 and Art 6.1.f GDPR legitimate interest of the controller or of a third party may be used as legal basis, also when the processing is carried out for marketing purposes. LSA argues the data subject did not present any prevailing fundamental rights and freedoms and neither are prevailing rights and freedoms apparent, as the data is already publicly accessible. As such, the aforementioned legal basis "can be considered as an allowing legal basis."

The original request of access and to erasure were filed before the 25 May 2018. Articles 13 and 14 GDPR were thus not yet applicable. However, under the GDPR the data subjects are to be informed from which source the personal data originate. The enterprise should be informed about this for future advertising mails".

Decision

The LSA deems this not be an infringement. The processing of publically available personal data for direct marketing purposes may constitute lawful processing according to Art 6.1.f GDPR.

Die Landesbeauftragte für Datenschutz und Informationsfreiheit
Fritz-Dobisch-Straße 12 • 66111 Saarbrücken

Die Landesbeauftragte für Datenschutz
und Informationsfreiheit

Fritz-Dobisch-Straße 12 • 66111 Saarbrücken
Postfach 10 26 31 • 66026 Saarbrücken
Telefon 0681 94781-0
Fax 0681 94781-29
E-Mail poststelle@datenschutz.saarland.de
Internet www.datenschutz.saarland.de
www.informationsfreiheit.saarland.de

[REDACTED]

Saarbrücken, 7 March 2019

Ref. No.: B 3800/181
Contact [REDACTED]
[REDACTED]

**Supervision pursuant to § 40 German Federal Data Protection Act (BDSG) in conjunction
with Art. 57 ff General Data Protection Regulation (GDPR)**

Subject: **Termination of proceedings**

Dear [REDACTED]

We refer to our letter dated 26 February 2019 in which we had requested your position on the complaint made by a [REDACTED], which was passed on to this office by the French data protection authority (CNIL) on the basis of Art. 56 General Data Protection Regulation (GDPR). In his complaint, the complainant asserted that he had asked you in two emails sent to [REDACTED] on 25 October 2017 and 14 November 2017 respectively to delete his account on [REDACTED] and on its servers. You allegedly did not respond to these erase requests.

You informed us that there were indeed data of the complainant still in existence and that you had failed to delete them, stating that the following data of the complainant were still stored: username, email address, the point in time at which the account was created, a password hash and an anonymous session ID to log into the website. You claimed that registering on [REDACTED] had no longer been possible since 2015, which is why you did not give adequate consideration to requests for support from old, already existing users. You informed us that, subsequent to receiving the letter sent by our office, the personal data of the complainant was immediately deleted and the complainant had also been notified thereof. You have apparently taken organisational measures to ensure that you take note of deletion requests promptly in the future so that they can also be processed within the statutory period permitted.

Within the scope of Art. 58 Subsection 2 of the GDPR, the supervisory authority has the power to decide whether further measures are to be taken in a particular case (so-called discretion in decision-making). In this case, I deem further measures by this office to be unnecessary, especially in consideration of the information which you have provided and the willingness to cooperate expressed in this respect. You complied with the request made by the complainant – after we had been brought it to your attention – and deleted the data. You have also taken appropriate measures to ensure that requests relating to the GDPR will be promptly processed in the future. Also to be taken into consideration was the fact that this was a first infringement. Moreover, the consequences for the person concerned of the delay in processing the deletion request were not serious as only less sensitive data of the person concerned were stored.



Finally, I would like to point out that we reserve the right to take further action if we receive additional complaints.

Yours sincerely
pp

[Redacted signature]



Summary Final Decision Art 60

Complaint

Closure of proceedings

Background information

Date of final decision:	7 March 2019
LSA:	DE -Saarland
CSAs:	DK, FR, NO, SE
Legal Reference:	Right to Erasure (Article 17), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12)
Decision:	Closure of proceedings
Key words:	Right to erasure, Exercise of the rights of data subjects

Summary of the Decision

Origin of the case

The complainant sent two emails to the controller requesting the deletion of this account on the controller's website and servers. The controller did not answer the request.

Findings

The data controller acknowledged that it had failed to delete the complainant's data, and proved that, following the inquiry sent by the LSA, the account was deleted. The controller also demonstrated that it had adopted appropriate organisational measures to ensure compliance with erasure requests in the future.

Decision

The LSA decided to not take further measures since the controller had acted promptly and had taken the appropriate measures to ensure the effectiveness of future requests related to the GDPR.



Berlin, 7 April 2020

FD 120406

Nat. Ref. Berlin DPA: 521.11521 / 632.212

IMI A56ID 71414

Nat.Ref. ICO: C-19-7-19

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

Sole subject of the complaint is an e-mail by which the controller informs the complainant that his personal data have been the subject of a data leak.

The controller has notified the Berlin DPA of the data breach pursuant to Art. 33 GDPR and notified the data subjects, including the complainant, according to Art. 34 GDPR. (Please see IMI A60DD 102273 for the draft decision about the notified data breach.)

The controller has informed the Berlin DPA that the cause of the loss of the data could not be finally determined. Both a hacker attack and unauthorised data access by employees could be considered.

Furthermore, the controller has announced that the affected servers have now been removed from the network and the data on them has been deleted. Shortly before the reported data protection violation, the controller switched to a more secure cloud service. The controller also increased the technical security measures in various aspects, which is why a reoccurrence of the incident is not to be expected.

For this reason, the Berlin DPA sees no reason to take any further measures against the controller.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

Summary Final Decision Art 60

Complaint

No infringement

EDPBI:DEBE:OSS:D:2020:99

Background information

Date of final decision:	7 April 2020
Date of broadcast:	9 April 2020
LSA:	DEBE
CSAs:	AT, DE, DK, ES, FI, FR, HU, IE, IT, NL, NO, SE
Controller:	Cardmarket / Sammelkartenmarkt GmbH & Co. KG
Legal Reference:	Personal Data Breach (Articles 33 and 34)
Decision:	No infringement
Key words:	Right to erasure, Deletion, Data retention

Summary of the Decision

Origin of the case

The controller sent an email to the complainant informing them that their data had been subject to a data leak. The controller notified the LSA of the data breach pursuant to Art 33 GDPR and notified the data subjects, including the complainant, according to Art 34 GDPR.

Findings

The controller informed the LSA that the cause of the loss of the data could not be finally determined. Both a hacker attack and an unauthorised data access by employees have been considered as causes of the breach.

The controller has announced that the affected servers have been removed from the network and the data stored on them has been deleted.

Decision

Due to the fact that the controller switched to a more secure cloud service just before the reported violation and increased technical security measures, a reoccurrence is not expected. For this reason, the LSA has not taken any further measures against the controller.



Berlin, 30 April 2020

535.1014
631.125
IMI A56ID 92258
DD 110613
FD 122414

Final Decision

1. Facts concerning the data breach

- **Controller:** Delivery Hero SE
- **Description of the data breach:** see 3.
- **Time and date of the incident:** 15 July 2019, 18:00 o'clock
- **Time and date of awareness of the incident:** 15 July 2019, 20:00 o'clock
- **Affected data subjects:** 1446 employees in the EEA, of which 1035 are in Germany
 - o Delivery Hero SE (Germany): 1035
 - o Click Delivery SA (Greece): 98
 - o Online Delivery AE (Greece): 43
 - o Delivery Hero Austria GmbH: 100
 - o Delivery Hero Finland: 24
 - o Foodora Finland Oy: 7
 - o Foodora AB (Sweden): 21
 - o Foodora Norway AS: 46
 - o Foodpanda Bulgaria Ltd: 40
- **Category of the data types/data records concerned:** login credentials for the in-house communication platform
- **Likely consequences of the violation of the protection of personal data:** Takeover of work-related platforms through password guessing

2. Measures taken by the LSA Berlin DPA

The case has been closed. In support of this, we refer to the statements under 3 - 6, where it is pointed out that the data subjects concerned were informed of the incident.

3. Cause of the data breach

Due to a faulty configuration of the development environment by an employee, a token for the in-house communication platform Slack was published on the Internet. Due to the publication of the token, personal data of the employees' login credentials were publicly accessible for a short time. The token was tested in the development

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

environment and was to be imported into Slack to make a technical change. This is where the error occurred.

4. Security measures taken by the controller at the time of awareness of the data breach

After the data protection violation became known, the token in question was immediately revoked. This meant that the contents of the token could no longer be accessed. Furthermore, all security measures were analysed again. No further vulnerabilities in the default settings could be identified.

5. Technical and organisational measures that the controller has taken to address the data protection violation

The Tech Department was assigned to another data protection and information security training course, which took place on 24 July 2019. In addition, random samples of the data published on the Internet were examined for publication. This would be an indicator that other people have seen and downloaded this data or forwarded it to other third parties.

6. Analysis of the effectiveness of these measures, especially with regard to prevent a new data breach in the future

Both the immediate measures taken (token deactivation) and the subsequent measures can be considered sufficient.

7. Examination of the underlying data protection violation

The case has been closed, as it is a minor violation due to a technical fault that is not expected to have serious consequences for the data subjects concerned.

The temporary publication of the information on the Internet can only have resulted in third parties gaining knowledge of who works for the controller and its subsidiaries. The technical error was quickly remedied; the responsible department received follow-up training in data protection law.

Further damage is not foreseeable for the time being, or can only be achieved with additional effort.

The company has contacted the Berlin Commissioner for Data Protection and Freedom of Information to report a violation of the protection of personal data. An unlawful processing of personal data has not taken place, since the token itself does not represent a personal datum, but can only provide access to this data like a key. There was therefore a security risk for the data concerned. Since, to our knowledge, this is not a structural defect or a problem that is likely to recur, we do not see any urgent need for action. Nor is the breach itself serious enough to warrant the imposition of a fine. As

this is not a complaint, we are not obliged to take any action against the company.

Summary Final Decision Art 60

Personal data breach notification

No sanction

EDPBI:DEBE:OSS:D:2020:103

Background information

Date of final decision:	30 April 2020
Date of broadcast:	30 April 2020
LSA:	DEBE
CSAs:	AT, BG SA, DEBY, FI, FR, NO, SE
Controller:	Delivery Hero SE
Legal Reference:	Security of processing (Article 32), 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:	No sanction
Key words:	Personal data breach, Data security

Summary of the Decision

Origin of the case

A token for the controller's in-house communication platform was published on the Internet due to a faulty configuration of the development environment by an employee. The publication of the token caused that personal data of the employees' login credentials for the in-house communication platform were publicly accessible for a short time. The data breach affected 1446 employees in the EEA. The data controller notified the breach to the LSA and to the data subjects concerned.

Findings

After the breach became known, the token in question was immediately revoked, rendering the contents of the token no longer accessible. Furthermore, all security measures were reviewed, and no further vulnerabilities in the settings could be identified.

The controller assigned a follow-up data protection and information security training course to the responsible department the week after the breach, and analysed random samples of the data

published on the Internet. The LSA considered these measures efficient and sufficient to remedy the breach caused by the technical fault and prevent future breaches.

The LSA found that the breach was a minor violation that was not expected to have serious consequences for the data subjects concerned as the temporary publication of the information could only have resulted in third parties gaining knowledge of who works for the controller. The LSA sustained that further damage was not foreseeable for the time being, or could only be achieved with additional effort. No unlawful processing of personal data had taken place, since the token itself does not represent personal data, but can only provide access to this data like a key.

Decision

The LSA decided to close the case on the ground that the breach did not point to a structural defect or a problem that is likely to reoccur. Moreover, the LSA came to the conclusion that there was no urgent need for action and that the breach was not serious enough to warrant the imposition of a fine.



Berlin, 28. April 2020

521.11540 / 631.144.1

A56ID 105454

CR 112682

DD 114100

FD 123064

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

Final Decision

Reprimand

To:
N26 Bank GmbH
Klosterstr. 62
10179 Berlin

Dear [REDACTED]
Dear [REDACTED]

We hereby reprimand your company for an infringement of the General Data Protection Regulation (GDPR) when processing personal data in your area of responsibility.

Justification:

Our decision is based on the following considerations:

I.

We have established the following facts:

On 1 June 2019, the complainant exercised his right to information under Article 15 GDPR. You only fulfilled the right to information after we wrote to you on 17 July 2019. The reason for the delay was the mistake of an individual employee. There has been a breach of Art. 12 (3) (1) GDPR (one-month period).

You have also transferred data about the complainant through the Facebook Custom Audiences program. This was done without consent and without a justifiable legal provision (see memorandum by [REDACTED] dated 19 September 2019).

II.

The reprimand is based on Art. 58 (2) (b) GDPR. There has been a violation of the GDPR in your area of responsibility.

Taking into account the specific circumstances of the facts of the case under investigation, we consider a reprimand to be appropriate following the conclusion of our investigation. With regard to the violation of Art. 12 GDPR, we have taken into account that this was the fault of an individual employee and that you further trained this employee. Regarding the transfer of data to Facebook, we refrained from initiating administrative offence proceedings only because you changed the procedure following our criticism.

In the safe expectation that you will comply with data protection regulations in the future, we consider the matter closed.

With kind regards,

Summary Final Decision Art 60

Complaint

Reprimand to controller

EDPBI:DEBE:OSS:D:2020:104

Background information

Date of final decision: 28 April 2020

Date of broadcast: 7 May 2020

LSA: DEBE

CSAs: AT, BE, all DE SAs, DK, ES, FR, IT, LU, NO, SI

Controller: N26 Bank GmbH

Legal Reference: Right of access (Art 15), Lawfulness of the processing (Art 6)

Decision: Reprimand to controller

Key words: Consumers, Right of access, reprimand

Summary of the Decision

Origin of the case

The controller failed to respond to the complainant's request for information within the one month period allotted under Article 12(3)(1) GDPR.

Findings

The request for information was only fulfilled once the controller was contacted by the LSA. The reason for delay was due to the mistake of an individual employee.

The controller also transferred the complainant's data without consent and justifiable legal provision, through the Facebook Custom Audiences program.

Decision

Taking the specific circumstances of the case, the LSA considered a reprimand to be the appropriate conclusion to the investigation. With regard to the transferring of data to Facebook, the LSA refrained from initiating administrative offence proceedings as the controller's procedure has been improved following the position of the LSA.



Berlin, 7 May 2020

521.10595
632.132
A56ID 54266
CR 54550
DD 111611
FD 123928

Final Decision

The DPA in Denmark had sent us a letter of complaint dated 1 July 2018, in which [REDACTED] objected to the sending of an unsolicited email. He claimed to have been a customer of www.care.dk. After the termination of the business relationship with care.com Europe GmbH, the complainant had requested the deletion of his personal data. The deletion of data was confirmed to him by e-mail. This e-mail was not provided to us.

The correspondence with care.com Europe GmbH, in which we also followed the reference number "ref: _00D708kOO_ _500391xa4yv:ref", was unsuccessful. It has been reported that a corresponding data record on [REDACTED] is not available at Care.com Europe GmbH. Thus, no data protection violation could be determined. Furthermore, it was also pointed out that www.care.dk appears to be an independent humanitarian organisation. This web address was mentioned in addition to www.care.com in the above-mentioned letter of complaint and has nothing to do with the company care.com Europe GmbH.

All attempts to clarify the facts of the case using only the information "first name and surname of the complainant" have been unsuccessful.

In the light of the above-mentioned considerations, the Berlin DPA has closed the case.

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

Summary Final Decision Art 60

Complaint

No violation

EDPBI:DEBE:OSS:D:2020:106

Background information

Date of final decision:	7 May 2020
Date of broadcast:	14 May 2020
LSA:	DE BE SA
CSAs:	DK, ES, FR, NO,
Controller:	Care.com Europe GmbH
Legal Reference:	Right to erasure (Article 17)
Decision:	No violation
Key words:	Right to erasure

Summary of the Decision

Origin of the case

Following the termination of the business relationship between the controller and the complainant, the complainant requested deletion of his personal data. The complainant received confirmation that his data had been deleted. Since then, the complainant allegedly received an unsolicited email. No proof of this has been made available.

Findings

The LSA followed up with the controller and was unsuccessful in finding a violation of the GDPR. It was also noted that one of the web addresses mentioned in the original letter of complaint was not affiliated with the controller by any means. Attempts to clarify the facts of the case using only the first name and the surname of the complainant have been unsuccessful.

Decision

In light of the above, the LSA found no violation of the GDPR.



Berlin, 10 June 2020

535.696
631.86
A56ID 74950
DD 109067
FD 131464

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

1. Facts concerning the data breach

- **Controller:** EyeEm Mobile GmbH (free online platform for sharing photos)
- **Incident:** Offering of personal data hacked at the controller in the dark net (Dream Market)
- **Time and date of the incident:** probably February 2018
- **Time and date of awareness of the incident:** 12 Feb. 2019
- **Concerned EU-/EEA-member states, each with the number of the affected data subjects:**
 - Germany: 54,440
 - Italy: 44,573
 - Spain: 24,232
 - United Kingdom: 24,169
 - France: 20,404
 - Poland: 9,973
 - Netherlands: 8,290
 - Portugal: 7,098
 - Austria: 6,327
 - Hungary: 5,379
 - Romania: 5,017
 - Sweden: 4,303
 - Belgium: 4,299
 - Czech Republic: 3,363
 - Greece: 3,254
 - Bulgaria: 2,496
 - Norway: 2,476
 - Lithuania: 2,459
 - Denmark: 2,354
 - Croatia: 1,888
 - Slovakia: 1,775
 - Finland: 1,561
 - Ireland: 1,342
 - Slovenia: 1,274
 - Latvia: 1,271
 - Estonia: 856

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

- Cyprus: 649
 - Luxembourg: 405
 - Malta: 295
 - Iceland: 180
 - Liechtenstein: 39
- **Category of data subjects:** customers
 - **Category of the data types/data records concerned:** names, e-mail addresses, user account data, encrypted passwords
 - **Likely consequences of the violation of the protection of personal data:** Disclosure and misuse of the above personal data

2. Description of the data breach from a technical-organizational point of view

An external security auditor (Mauer IT Consulting) identified two possible security vulnerabilities for the data breach: outdated OpenVPN server version, open SSH ports.

3. Description and analysis of the effectiveness of the measures taken to address the data breach or mitigate its adverse effects (Art. 33 (3) (d) GDPR)

The passwords of affected users were blocked and access tokens (access authorizations created for the respective applications of the users) were deleted. The password hash procedure was changed to Bcrypt. In addition, the security vulnerabilities described under 2. were closed.

These measures will prevent the exploitation of the security gaps found for the future. By resetting all access credentials, the attacker is prevented from further access to accounts that have already been taken over. The measures are considered to be sufficient.

4. Communication to the concerned data subjects or public communication (Art. 34 (1) or Art. 34 (3) (c) GDPR)

The persons concerned were informed about the incident by the controller in several stages, i.e. by two e-mails (in English). In addition, a data protection statement (German/English) was placed on the website of the controller (following our recommendation at least until the end of May 2019).

5. Technical and organisational measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

Even before the incident, a salted hash method was used, although SHA1. A bulk decryption of the passwords is therefore more difficult.

6. Subsequent measures by which the controller has ensured that a high risk to the concerned data subjects is no longer likely to materialise (Art. 34 (3) (b) GDPR)

See 3.

7. Taken measures by the LSA Berlin DPA

Taking the specific circumstances of the facts determined into account, the Berlin DPA considers the case closed in regard to Art. 33 and Art. 34 GDPR.

Moreover, the Berlin DPA issues a reprimand to the controller with regard to the underlying data protection violation (see attached letter).

Summary Final Decision Art 60

Legal obligation

Reprimand to controller

EDPBI:DEBE:OSS:D:2020:114

Background information

Date of final decision:	10 June 2020
Date of broadcast:	16 June 2020
LSA:	DEBE
CSAs:	All SAs
Controller:	EyeEm Mobile GmbH
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	Reprimand to controller
Key words:	Consumers, Data breach, E-commerce

Summary of the Decision

Origin of the case

The case originated from a data breach notification. The controller was made aware of the breach through a media report that there had been a cyberattack on their platform. According to the media report, user's personal data was obtained without authorisation and was being sold on the dark net. The personal data included names, email addresses, user account data and encrypted passwords.

Findings

As part of the measures taken to address the data breach as reported to the LSA, an external security auditor identified two possible security vulnerabilities. The vulnerabilities included an outdated OpenVPN server version and open SSH ports, which probably enabled the attack that caused the data breach.

Decision

The reprimand is based on Art 58(2)(b) GDPR. According to Art. 32 GDPR, a controller must implement appropriate technical and organisational measures to ensure a level of protection appropriate to the risk. By using insufficiently updated software and an insufficiently secured configuration of IT systems, these requirements were not met.

Taking the specific circumstances of the facts determined into account, a reprimand was considered appropriate following the completion of the investigation. This is the controller's first Art 32 GDPR violation and it has now resolved the security vulnerabilities.



Berlin, 13 July 2020

Berlin Commissioner for
Data Protection and
Freedom of Information

631.184.2
535.1133
A56ID 109329
DD 129684
FD 135781

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** Xara GmbH
- **Incident:** Hacker attack on email account
- **Date of occurrence:** 16 August 2019
- **Date of acknowledgement of the incident:** 5 September 2019
- **EU/EEA Member States concerned, with the number of data subjects concerned:**
 - o Establishment in Germany: 17
 - o Establishment in UK: 20
 - o Data subjects who are employed both in Germany and the UK (in home-office): 16
- **Category of data subjects:** Employee data
- **Category of the data types/data records concerned:** First name, surname, email-address
- **Likely consequences of the violation of the protection of personal data:** data misuse

2. Description of the data breach from a technical-organizational perspective

It is highly probable that unknown persons captured Office365 account login data via an e-mail containing modified hyper-links. Utilising this login data, they created an administrator account and gained access to the e-mail accounts of several employees. Afterwards fake e-mails were sent.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

Once the activities were detected, the passwords of all accounts, including accounts with other services, were changed and a multi-factor authentication was immediately activated for accounts with access to sensitive data (including all employees in the finance department). As a further measure,

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

the introduction of multi-factor authentication for all accounts is planned. In addition, all affected workstations were subjected to a virus scan.

The technical measures are considered to be effective, since login data is much more difficult to be misused when multi-factor authentication is activated.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

All data subjects concerned were notified on 6 September 2019 via email.

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

Standard Microsoft security features for Office 365, no multi-factor authentication.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

As a further measure, the introduction of multi-factor authentication for all accounts is planned.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has not identified any data protection violations beyond Articles 33, 34 GDPR.



Berlin, 13 July 2020

631.87
535.699
A56ID 74975
CR 82038
RD 129527
FD 135778

**Berlin Commissioner for
Data Protection and
Freedom of Information**

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to
disabled members of the public.

Contact us

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

Use our encrypted contact form
for registering data protection
complaints:
www.datenschutz-berlin.de/be-schwerde.html

For all other enquiries, please
send an e-mail to:
mailbox@privacy.de

Fingerprint of our
PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to
Kochstraße / Bus number M29
and 248

Visit our Website

<https://privacy.de>

1. Facts concerning the data breach

- **Controller:** Dubsmash Inc. / Mobile Motion GmbH (Software) as sole branch in EU/ EEA
- **Incident:** Offering of personal data hacked at Dubsmash in the Darknet (Dream Market)
- **Time and date of the incident:** unknown
- **Time and date of awareness of the incident:** 8. Feb. 2019
- **Concerned EU-/EEA-member states, each with the number of the affected data subjects:**
 - o United Kingdom: 2860348
 - o Germany: 2044890
 - o Spain: 1624919
 - o Italy: 1558241
 - o Greece: 703880
 - o Czech Republic: 647773
 - o Romania: 592149
 - o Hungary: 508958
 - o Poland: 402999
 - o The Netherlands: 378192
 - o Belgium: 354687
 - o Sweden: 275121
 - o Austria: 229702
 - o Finland: 223663
 - o Portugal: 220004
 - o Slovakia: 203469
 - o Ireland: 179079
 - o Norway: 174624

- Denmark: 125390
- Croatia: 105163
- Bulgaria: 92405
- Slovenia: 54019
- Lithuania: 50308
- Cyprus: 40440
- Latvia: 36338
- Estonia: 12952
- Luxembourg: 11938
- Iceland: 10423
- Malta: 9954
- Gibraltar: 1369
- Liechtenstein: 596
- France: 1965728
- French Southern Territories: 6
- Vatican: 10

- **Category of data subjects:** Dubsmash users
- **Category of the data types/data records concerned:** User names, passwords, date of birth, telephone number, e-mail addresses and country/language information, if provided by the user
- **Likely consequences of the violation of the protection of personal data:** Disclosure and misuse of the above data

2. Description of the data breach from a technical-organizational point of view

The reason why the attackers were able to steal user data and publish it in the darknet could not be determined, partly because no access logs were available at the service provider in the affected period. The compromised database was stored with the Cloud-Hoster Heroku. The access logs to backup data showed no abnormalities. In addition, penetration tests were carried out.

3. Description and analysis of the effectiveness of the measures taken to address the data breach or mitigate its adverse effects (Art. 33 (3) (d) GDPR)

The company hired a forensics firm to identify network vulnerabilities, but this was unsuccessful for the reasons mentioned above. In addition, log-in credentials were changed and access controls were reviewed.

4. Communication to the concerned data subjects or public communication (Art. 34 (1) or Art. 34 (3) (c) GDPR)

The concerned data subjects were informed of the incident in writing on 14 February 2019. In addition, press releases were published on the same day (in several languages).

5. Technical and organisational measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

The stolen passwords were hashed with PBKDF2-SHA 256 using salt values. A disclosure of the unencrypted passwords on a large scale is therefore hardly possible even with knowledge of the database.

6. Subsequent measures by which the controller has ensured that a high risk to the concerned data subjects is no longer likely to materialise (Art. 34 (3) (b) GDPR)

Among others, the controller:

- carried out investigations on access control, examining user-accounts and rights management. Access to the authoritative postgres database via the cloud provider's CU was limited to three Dubsmash employees, each of whom has their own personalized accounts.
- performed forensic examinations of logs, including from Amazon AWS, CloudTrail, Postgres SQL and GitHub, for hints on a possible access to data and their transmission during the period of the alleged data leaks.
 - The Postgres SQL protocols were not available for the November 2018 timespan;
 - The CloudTrail protocols for potential access to the S3-Bucket for the backup of the database showed no accesses and no Data transmissions with regard to the data stored there.
 - The EC2B Backup log information showed for the period of 6. January (only from this date protocols were available) to February 9 (date of analysis) no unauthorised access; no protocol data for November 2018 were available anymore, because the data sets had already been changed by the Linux operating system.
 - The GitHub log analysis showed that there were no suspicious user activities that could lead to unauthorized data transfer from the Postgres database.

Users were advised to change their passwords regularly and to avoid the cross-platform use of passwords. The company has also pointed out additional security measures to prevent the porting of telephone numbers.

A 2-factor authentication was introduced for relevant services. In addition, it is now ensured that all internal communication channels are also TLS encrypted. Also, organisational measures have been taken to ensure that all software components are kept up-to-date on a permanent basis.

7. Measures by the LSA Berlin DPA

Against the background of above considerations regarding Art. 33 and 34 GDPR the Berlin DPA closes this investigation.

Furthermore, the Berlin DPA has not identified any data protection violations.

Summary Final Decision Art 60

Legal obligation

No violation

EDPBI:DEBE:OSS:D:2020:124

Background information

Date of final decision:	13 July 2020
Date of broadcast:	14 July 2020
LSA:	DEBE
CSAs:	All SAs
Controller:	Dubsmash Inc / Mobile Motion GmbH
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No violation
Key words:	Consumers, data breach, social media

Summary of the Decision

Origin of the case

The controller notified the LSA of the data breach having been made aware of a data dump for sale on the internet by an investigative reporter. The controller immediately launched an investigation and could verify the content of the database as being the controller's data. The data dump contained users' public information such as usernames, first and last names, photos and encrypted passwords. Some users also supplied additional private information that is believed to be part of the affected data: email, birth dates, phone numbers, device country/ language information and profile pictures.

Findings

The reason why the attackers were able to steal user data and publish it on the darknet could not be determined, partly because no access logs were available. The access logs to backup data showed no abnormalities. In addition, penetration tests were carried out. The controller hired a forensics firm to identify network vulnerabilities, but this was unsuccessful for the reasons mentioned above. Log in credentials were changed and access controls were reviewed.

The concerned data subjects were informed of the incident and press releases were published on the same day.

The controller has taken a large number of subsequent measures to ensure that a high risk to the concerned data subjects is no longer likely to materialise including investigations on access control and performing forensic examinations of logs. Users were advised to change their passwords regularly and to avoid the cross-platform use of passwords and two factor authentication has been introduced for relevant services.

Decision

Considering the above, the LSA has closed its investigation. The LSA has not identified any data protection violations.

Summary Final Decision Art 60

Legal obligation

No violation

EDPBI:DEBE:OSS:D:2020:125

Background information

Date of final decision:	13 July 2020
Date of broadcast:	14 July 2020
LSA:	DEBE
CSAs:	DE, UK
Controller:	Xara GmbH
Legal Reference:	Personal data breach (Articles 33 and 34)
Decision:	No violation
Key words:	Data breach

Summary of the Decision

Origin of the case

The controller reported that the log-in information of an email account was obtained, likely through an email containing modified hyperlinks. Utilising those log in data, an administrator account was fabricated and used to send/receive emails in order to forge billing emails.

Findings

Once the activities were detected, the passwords of all accounts, including accounts with other services, were changed and a multi-factor authentication was immediately activated for account with access to sensitive data (including all employees in the finance department). Multi-factor authentication is planned for all accounts in the future. All affected workstations were subjected to a virus scan.

All data subjects concerned were notified of the breach via email.

Decision

In light of the above, the LSA has closed the case and has not identified any data protection violations beyond Articles 33 and 34 GDPR.

Pandora A/S
Havneholmen 17-19
1561 Copenhagen V
Denmark

25 October 2019

J.No. 2018-7320-0166
Doc.no. 137612
Caseworker
[REDACTED]

Sent with Digital Post

Complaint about processing of personal data

The Danish Data Protection Agency returns to the case where, on the 30th of May 2018, [REDACTED] [REDACTED] (hereinafter: the complainant) complained to the Information Commissioner's Office (ICO) that Pandora A/S (hereinafter: Pandora) has refused to delete his personal data in Pandora's systems/databases. In line with Article 56 of the General Data Protection Regulation¹, the Danish Data Protection Agency has been designated as the leading supervisory authority of the case.

The Danish Data Protection Agency
Borgergade 28, 5.
1300 Copenhagen
Denmark
T 3319 3200
dt@datatilsynet.dk
datatilsynet.dk
VAT No. [REDACTED]

1. Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds to **criticize** that the processing of personal data by Pandora has not been done in accordance with the rules of Article 12(6) and Article 5(1)(c) of the General Data Protection Regulation.

The Data Protection Agency also finds basis to **order** Pandora in the complainant's case to make a decision whether the conditions for erasure under Article 17 of the General Data Protection Regulation have been met and, if so, to delete the personal data processed about complainant. The decision shall be taken as soon as possible and **no later than two weeks from the date of this letter**. The order is granted pursuant to Article 58(2)(c) of the General Data Protection Regulation.

The Data Protection Agency draws attention to the fact that, pursuant to Paragraph 41(2)(5) of the Data Protection Act², failure to comply with an order issued by the Danish Data Protection Agency pursuant to Article 58(2)(c) of the Regulation is punishable.

Pandora is requested to notify the agency when a decision has been made.

The details of the case and the reasons for the decision of the Danish Data Protection Agency are set out below.

¹ Regulation (EU) 2016/679 Of The European Parliament And OF The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

² Act No. 502 of 23 May 2018 on supplementary provisions to the regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

2. Statement of facts

Page 2 of 7

On the 23th of May 2018 the complainant contacted Pandora by e-mail and requested to be deleted from the company's database.

In an e-mail of the 29th of May 2018, Pandora requested that the complainant submit his request to be deleted via the company's online form.

The complainant then completed the online form on the same day, but due to technical problems, the complainant took some screenshots of the completed form and sent the images of the completed form to Pandora via e-mail.

On the 30th of May 2018 Pandora informed the complainant that in order to process his request for deletion he had to submit proof of identification in the form of, for example, passport, driving license or national identity card, in order to confirm his identity, in accordance with the requirements of the online form on the website.

However, the complainant did not wish to send proof of identity to Pandora. Therefore, the complainant's request for deletion was not granted since, in Pandora's opinion; Pandora was not able to identify the complainant with certainty without proper identification.

2.1. Pandora's remarks

Pandora has stated that the data subject fills in the form on the Pandora homepage, which is sent encrypted to Pandora, after which it is stored in Pandora's internal systems and is handled and answered by a designated employee. As the data subject can enter any e-mail address in the form, including one which is not registered in Pandora's systems, the data subject will after submitting his/her request immediately receive a confirmation e-mail from Pandora with a link to be used to confirm the request.

Pandora has also stated that if the data subject enters an e-mail address that is not registered in the company's systems, or there are other uncertainties regarding the request, Pandora's customer service department contacts the data subject for clarification.

Once the request has been answered, Pandora will confirm this to the data subject and the proof of identification attached to the form will be deleted immediately after the application has been handled. The proof of identification will not be stored more than 30 days, unless the request is extended pursuant to Article 12(3).

Pandora has stressed that the proof of identity of the data subject is exclusively used for identity purposes, and that Pandora will never ask for identification in connection with requests that relate only to the data subject's wish to be deregistered as recipient of a Pandora newsletter (which he/she has registered for).

Pandora has indicated that ID validation is an important part of Pandora's DSR procedure (data subject rights procedure). In the case of Pandora, the company is obliged to verify the identity of the data subject before a DSR request is handled. In particular, Pandora has referred to recital 64 of the General Data Protection Regulation, the Danish Data Protection Agency's guidance on data subjects' rights section 2.6 and report No 1565 on point 4.2.2.4 of the Data Protection Regulation.

Pandora has stated that it has around 9,7 million registered customers and Pandora does not have a unique identifier (e.g. customer or ID number) for each customer that can be used to validate the customer's identity. The personal data, if any, recorded by Pandora in the company's systems (e.g. name, address, e-mail address, phone number), according to Pandora

are easy to look up on social media and the information is, to some extent, publicly available. It is Pandora's view that a procedure in which Pandora does not request proof of identity would entail a significant risk for Pandora's customers.

Page 3 of 7

Pandora states that, in the opinion of Pandora, the company's procedure fulfils the condition that the assessment of whether proof of identity is to be considered necessary must be assessed on a case-by-case basis in relation to the individual request. Pandora argues in this respect that because the relationship of Pandora to its customers is primarily an online environment in which the company does not know the natural person behind the request, the individual assessment will be the same in each case. Therefore, in the opinion of Pandora, there will either always be a reasonable doubt and a general risk, or there will be no reasonable doubt or a general risk.

In view of this complexity, Pandora initially carried out a risk assessment of the existing set up of the company and established on this basis a procedure which, in the opinion of Pandora, meets both the rights of the data subjects in an easy and secure manner, while Pandora observed the undertaking's obligations under the General Data Protection Regulation including the requirements set out in Article 12(2) and (6), as well as the obligation for the company to guarantee the data subjects' identity and not to unjustifiably provide or delete any personal data.

Pandora has argued that, in the present case, a specific assessment is not possible because there is no concrete information in the case that can be used as valid evidence to assume that the data subject is the person he claims to be. Pandora claims that, in the specific case, the request for proof of identity is necessary and proportionate.

In addition, Pandora has referred to the fact that the ICO on the 4th of December 2018 made a decision in a case that is by substance identical to the present one. The ICO did not find, in that case, grounds for criticizing the fact that Pandora had requested a customer to send proof of identity in order to validate his/her identity prior to processing the request for deletion by the customer. The ICO considered the request for identification to be proportionate.

2.2. The complainant's remarks

The complainant has generally stated that he did not want to give Pandora further personal data in order to have his deletion request processed. The complainant also claims that Pandora could have contacted him by e-mail or telephone in order to confirm his identity.

3. Justification for the Danish Data Protection Agency's decision

It follows from Article 12(2) of the General Data Protection Regulation that the controller should facilitate the exercise of the data subject's rights pursuant, inter alia, to Article 17 on erasure.

Under Article 12(6) of the General Data Protection Regulation, a controller may, if there is reasonable doubt as to the identity of the natural person making a request, demand additional information necessary to confirm the identity of the data subject.

It also follows from the principles relating to processing of personal data provided by the General Data Protection Regulation that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in accordance with Article 5(1)(c).

"There are no prescriptive requirements to be found in the GDPR on how to authenticate the data subject. (...) Additionally, Article 12(6) provides that where a data controller has reasonable doubts about the identity of a data subject, it can request further information to confirm the data subject's identity. (...) Where information and data collected online is linked to pseudonyms or unique identifiers, data controllers can implement appropriate procedures enabling an individual to make a data portability request and receive the data relating to him or her. In any case, data controllers must implement an authentication procedure in order to strongly ascertain the identity of the data subject requesting his or her personal data or more generally exercising the rights granted by the GDPR.

These procedures often already exist. The data subjects are often already authenticated by the data controller before entering into a contract or collecting his or her consent to the processing. As a consequence, the personal data used to register the individual concerned by the processing can also be used as evidence to authenticate the data subject for portability purposes.

While in these cases, the data subjects' prior identification may require a request for proof of their legal identity, such verification may not be relevant to assess the link between the data and the individual concerned, since such a link is not related with the official or legal identity. In essence, the ability for the data controller to request additional information to assess one's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.

In many cases, such authentication procedures are already in place. For example, user-names and passwords are often used to allow individuals to access their data in their email accounts, social networking accounts, and accounts used for various other services, some of which individuals chose to use without revealing their full name and identity."

The Danish Data Protection Agency assumes that Pandora always requests proof of identity from a data subject when a data subject wishes to exercise his/hers rights.

On the basis of a review of the case, the Danish Data Protection Agency finds that Pandora's general procedure, under which ID validation is required without exception when processing a requests to exercise the rights of the data subjects, is not in conformity with Article 12(6) and Article 5(1)(c) of the General Data Protection Regulation.

The Danish Data Protection Agency has attached importance to the fact that Article 12(6) of the General Data Protection Regulation requires the controller to carry out a specific assessment as to whether or not there are reasonable doubts as to the identity of the individual in relation to the individual application for the exercise of the rights of the data subject. The Danish Data Protection Agency considers in this context that the fact that there is an online customer relationship does not mean that there will always be reasonable doubts about the identity of the natural person.

³ During its first plenary meeting the European Data Protection Board endorsed the GDPR related WP29 Guidelines, including wp242rev.01.

The Danish Data Protection Agency has also emphasized that a request for additional information for the purpose of identifying the natural person should be proportionate in accordance with Article 5(1)(c) and, therefore, the controller should not request more information than is necessary for the identification of the natural person. The Danish Data Protection Agency finds that it is not in accordance with Article 12(2) that Pandora has organized a procedure whereby the data subject must provide more information than initially collected in order to have a request for the exercise of the rights of the data subject processed.

The fact that Pandora has failed to set up its systems in such a way that, for example, unique identifiers are attached to data subjects, cannot justify that Pandora requires, in all cases, that the data subject provides proof of identification in order to be able to exercise his/hers rights under the regulation. In the view of the Danish Data Protection Agency, Pandora's overall procedure for ID validation goes beyond what is required and makes it unnecessarily burdensome for the data subject to exercise his/her rights.

On the basis of the above, the Danish Data Protection Agency **criticizes** that the processing of personal data by Pandora has not been done in accordance with the rules of Article 12(6) and Article 5(1)(c) of the General Data Protection Regulation.

The Data Protection Agency also finds basis to **order** Pandora in the complainant's case to make a decision whether the conditions for erasure under Article 17 of the General Data Protection Regulation have been met and, if so, to delete the personal data processed about complainant.

The Danish Data Protection Agency notes that the agency in its handling of complaints will always carry out a specific assessment of the facts. In the view of the agency, a reference to a decision taken in another European country cannot necessarily lead to a corresponding decision being taken by the agency.

4. Final remarks

The Danish Data Protection awaits notification from Pandora. The notification must be received within two weeks of today's date.

The Data Protection Agency has informed the ICO of the decision in order for the ICO to pass on the decision to the complainant.

It should be noted that the Data Protection Agency expects to publish this decision on the agencies website.

Kind regards

[REDACTED]

Appendix: Legal basis

Appendix: Legal Basis

Extracts from Regulation (EU) 2016/679 Of The European Parliament And OF The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 5. Personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that accurate, having regard to the purposes for which they are processed, are erased or rectified without delay 'accuracy');
- e) 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');
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Article 12. 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

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.

Summary Final Decision Art 60

Complaint

Order to take a decision regarding the fulfilment of the conditions for erasure under Article 17 GDPR

Background information

Date of final decision:	25 October 2019
LSA:	DK
CSAs:	AT, BE, CY, DE, ES, FI, FR, HU, IT, LU, NL, NO, SE, SK, UK
Controller:	PANDORA A/S
Legal Reference:	Principles relating to processing of personal data (Article 5), Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12), Right to erasure (Article 17)
Decision:	Order to take a decision regarding the fulfilment of the conditions for erasure under Article 17 GDPR and a reprimand to the controller.
Key words:	Right to erasure, Data subjects' rights, Transparency

Summary of the Decision

Origin of the case

The complainant requested to have his personal data deleted from the controller's database. The controller replied that, before processing his erasure request, a proof of identification was necessary to confirm his identity. As the complainant refused to comply with the controller's demand, his data were not deleted.

Findings

The LSA found that the controller's procedure under which ID validation was required without exception when processing a data subject's request was not in conformity with Article 12(6) and Article 5(1)(c) GDPR. The LSA also found that, under the controller's procedure, data subjects had to provide more information than initially collected in order to have their request processed. Consequently, the controller's procedure for ID validation went beyond what was required and made burdensome for data subjects to exercise their rights.

Decision

The LSA criticized that the processing by the controller had not been done not in accordance with Article 12(6) and Article 5(1)(c) GDPR. It ordered the controller to decide within two weeks whether the conditions for erasure present in Article 17 GDPR were met and, if so, delete the complainant's data.

Summary Final Decision Art 60

Complaint

Dismissal of the case

Background information

Date of final decision:	5 February 2020
LSA:	DK
CSAs:	DE-Schleswig-Holstein, FR, SE
Controller:	Garnio ApS/ Hobbii Aps (Garnio ApS changed its name on 8 April 2019).
Legal Reference:	Right of access by the data subject (Article 15), Security of processing (Article 32), Personal data breach (Articles 33 and 34), and Tasks of the Data Protection Officer (Article 39).
Decision:	Dismissal of the case
Key words:	Data breach, security

Summary of the Decision

Origin of the case

The complainant requested access to his data processed by the controller. As a result of this request, the controller provided the personal data of another individual. The complainant contacted the controller again about the breach but the controller did not reply to the inquiry.

Findings

The LSA found that the data subject in this case was not entitled to complain, as the processing of personal data did not relate to that individual.

Decision

The LSA took notice of the security issue and the occurred breach of personal data. This will be taken into consideration during the planning of audits.



FOR INTERNAL USE

Holder of Information: Estonian Data Protection

Inspectorate

Notation made: 29 July 2019

Access restriction is valid until: 29 July 2094

Basis: clause 35 (1) 12) of the Public Information Act

Dear [REDACTED]

Ref.: 13 March 2019

[REDACTED]

Ref.: 29 July 2019 No. 2.1.-1/19/483

Notice of termination of the proceeding in regard to the protection of personal data

Proceedings are closed at the E [REDACTED] rotection Inspectorate concerning the complaint you submitted on the activities of [REDACTED] (hereinafter [REDACTED]). In your complaint, you pointed out that your personal [REDACTED] n transferred [REDACTED] d party on [REDACTED] (hereinafter [REDACTED]) without a legal basis to do so.

The Data Protection Inspectorate initiated a national supervisory review proceeding concerning the data controller. In their reply, the controller has confirmed that they have forwarded your personal data lawfully:

The person was a client of [REDACTED] who ordered [REDACTED] by signing a service provision contract with the [REDACTED] on 27 July 2012. On 13 July 2018, the client sent an application for the termination of the contract to t [REDACTED]. At the end of the contract, the client owed a debt of 14.73 euros to the [REDACTED] n 25 August 2018, 8 August 2018 and 22 August 2018, messages were sent to the client as reminders (Annex 1) of the debt, including information on how to pay the debt. On the two following occasions, on 31 August 2018 and 16 October 2018, we explained that if the debt is not paid, the debt claim will be forwarded to the claimant [REDACTED]

Clause 12.3 of the Contract concluded with the client stipulates that the [REDACTED] has the right to transfer, without consent from the client, its contractual rights an [REDACTED] ions to third parties, if that the transfer does not adversely affect the rights of the client. The client's rights have not been impaired, as it was agreed upon, during the conclusion of the contract, that the client will be provided a service and the [REDACTED] shall receive a fee for the provision of the service. If the debt for the service remains [REDACTED] he service provider has the right to demand the payment of debt, with which the client had to take into account when signing the contract.

The client has also agreed to the privacy policy of [REDACTED] (clause 12.4 of the contract stipulates that the [REDACTED] will process personal data in [REDACTED] nce with the privacy policy), which clearly states that, in order to perform the contract concluded with the client (Article 6 (1) (b) of the General Data Protection Regulation), we use the client's data, inter alia, in the event of a delay in the fulfilment of a financial obligation arising from the client's contract to provide information concerning the client and their debt (given name, surname, personal identification code, amount of debt, delay time, creditor, etc.) to the processor of the credit database and/or persons handling debts and, in the case of assignment of the right of claim, to a new creditor. The data will be forwarded for the purpose of disclosure in the relevant credit register. If the client has liquidated their debt, they have the right to demand that the respective persons terminate the processing of the client's personal data.

In addition to provisions concerning the disclosure of data, the privacy policy also stipulated that we can use third party enterprises who provide services to us, e.g. who provide infrastructure and IT services (incl. storing data, forwarding of data, monitoring quality), process credit card transactions, provide customer service, carry out recovery of debts, collect data for debt analysis and improvement of data, as well as concerning client inquiries, and conduct other statistical analyses. These enterprises may have access to client data in order to provide their services. We do not authorize these companies to use or disclose the client's personal data, except in order to provide the services we require.

The invoices submitted to the client (attached to the letter of the Lithuanian Data Protection Inspectorate) also state that if the invoice is not paid, the procedure for claiming payment of the invoice will be forwarded to [REDACTED]. Therefore, the [REDACTED] has repeatedly stressed in the contract, privacy policy, invoice [REDACTED] en reminding [REDACTED] bt, that if the debt is not paid, the claim procedure will be forwarded to [REDACTED]. The client failed to pay the debt, after which the [REDACTED] transferred the debt to the da sor, in this case to [REDACTED]. In a letter of debt rec t by [REDACTED] to the person, it has also been explained th [REDACTED] will process the person's person accordance with the contract concluded wit [REDACTED] and based on legitimate interest for the purpose of recovering the debt.

Concerning the appellant, the following data was provided to [REDACTED] client number, plan, personal identification code, first name, surname, address, e-mail [REDACTED], mobile number, time of conclusion of the contract, date and manner of sending the reminders of arrears, invoice details, debt.

The [REDACTED] has compiled a privacy policy (data processing principles), which is accessible on t [REDACTED] A sample of the contract can be [REDACTED]

Separately, the data controller informed the Inspectorate that the appellant had not approached them directly. The Inspectorate explains that, in general, with regard to procedural economics, only those complaints where the parties have not reached an agreement with each other or the person has not received a reply to their inquiry should be sent to the Inspectorate.

The Inspectorate also explains that with regard to processing of personal data, it only assesses whether the transfer of personal data has been lawful, not the lawfulness of the debt claim. The Estonian Data Protection Inspectorate does not have the competence to assess whether the debts of individuals against the creditor have arisen lawfully, what the claims consist of, whether or not the debt has actually been liquidated, whether or not the rules for the assignment of the claim have been complied with, as those are disputes that arise from contractual relations. Settlement of contractual disputes between private parties is a matter for the civil court. Law enforcement agencies cannot and are not obligated to be unable to identify the actual legal relationships between individuals, in each case, which may be very difficult when resolving in private disputes.¹ If the appellant finds that the creditor has violated the law in concluding, executing or assigning loan agreements, they have the right to bring the action before the court.

A similar conclusion was reached by the Tallinn Administrative Court on 22 March 2011 in its judgment No 3-10-994. In that judgment, the court held that the Data Protection Inspectorate had no legal competence to settle disputes arising from contractual relations, including the assessment thereof. The court noted that the Data Protection Inspectorate is a supervisory authority of the state that is competent to monitor compliance with the Personal Data Protection Act and legislation established on the basis thereof, and to conduct proceedings of the violations arising therefrom.

The Inspectorate has established that the person has been informed in the contract that was concluded with them that their personal data will be transferred upon the occurrence of a debt. The contract of personal data proces g t General Data Protection Regulation has been signed between [REDACTED] and [REDACTED]. In addition, the privacy policy also includes information reg issi the name of a particular legal entity is indicated in the invoices provided to the client. With this, the data controller has fulfilled every possible obligation to inform the person.

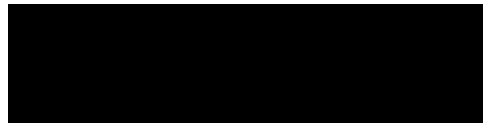
The transmission of data for the recovery of debt claims is a common practice for large enterprises and had to be acknowledged by the individual at the time of concluding the contract; same applies to the fact that the parties are able to settle any contractual disputes that they are not able to resolve among themselves in the court.

Inspection did not identify any violations by the data controller, and the national supervisory review proceeding is therefore terminated.

1 Page 20 of the explanatory memorandum of the Draft of the Law Enforcement Act.

According to [Administrative Procedure Act](#) article 75 a challenge concerning an administrative act or measure shall be filed within thirty days as of the day when a person becomes or should become aware of the challenged administrative act or measure.

Kind regards



Summary Final Decision Art 60

Complaint

No violation

EDPBI:EE:OSS:D:2019:30

Background information

Date of final decision: 2 August 2019

LSA: EE

CSAs: LT

Legal Reference: Articles 6 (Lawfulness of processing) and 13 GDPR (Information to be provided to the data subject)

Decision: No violation

Key words: Lawful processing, legal basis, third party, transfer of personal data

Summary of the Decision

Origin of the case

The data subject complained that the controller transferred his personal data to a third party, without having a legal basis to do so. The controller explained that provided a service to the complainant based on a contract. The complainant, who requested the termination of his contract, had accumulated a debt, which needed to be paid. Based on the said contract, if the client (i.e. the complainant) did not pay the debt, then the debt claim would be forwarded to the third party.

Findings

The LSA found the transfer of personal data was done lawfully; the complainant had been informed through the contract that his personal data would be transferred upon the occurrence of a debt. Furthermore, the privacy policy, available on the controller's website, included information on the transmission of data and the name of the third party.

Decision

The LSA did not find any violations by the data controller and closed the case.



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

FINAL DECISION

[REDACTED]

[REDACTED]

[REDACTED]

Reprimand for failure to comply with the requirements of the General Data Protection Regulation

Notice of termination of proceedings in a matter concerning the Electronic Communications Act

A complaint from person [REDACTED] and perso [REDACTED] forwarded by the French supervisory authority is currently processed by the Estonian Data Protection Inspectorate. [REDACTED] has carried out an investigation within your company due to an inquiry from the Estonian Data Protection Inspectorate.

During the proceedings, you responded to the Inspectorate's inquiries as follows:

Yes, the [REDACTED] is a self-employed person engaged in the relevant economic and professional activities, and the necessary registration [REDACTED] is required.

The persons who filed the complaint had joined the [REDACTED] platform as persons carrying out economic and professional activities.

- a) [REDACTED] provides service as a person engaged in economic or
- b) [REDACTED] provides service on [REDACTED] platform through the following company: [REDACTED]

For internal investigation, we need additional information about the time of sending the forwarded text messages in order to send the relevant inquiry to the partner whose channels were used to forward the messages. We have informed and communicated with the partner about this case.

For information, [REDACTED] usually sends two types of messages [REDACTED]:

A request for terminating the registration is sent if it is pending due to the submission of documents. We invite [REDACTED] when demand increases and [REDACTED]

correctly as it should be, the number should also have immediately reached the message blocking list. There is no information on when messages were exchanged and when the STOP inquiries were made.

All communication towards the [REDACTED] is related to the provision of services within economic and professional activities, in order to perform the contract.

We confirm that the account of [REDACTED] has been deactivated and unnecessary personal data has been deleted as of 2018-08-26.

The partner has been informed about the text message received with the STOP content. An investigation is ongoing with the partner and we expect to receive a response by 26/06/2019.

We have received from our data processor an extract about the operations performed on these numbers.

The messaging service provider of [REDACTED] said that the situation arose due to technical limitations, where the processing of the STOP message was implemented only with regard to one account (from where the message was sent) in their internal system but was not implemented with regard to the global number. The service provider is resolving the matter, so that when the client sends a STOP message, it would be implemented across accounts. Until the service provider implements the updates in the system, [REDACTED] uses accounts at the relevant service provider without global numbers.

Of the two documents added to the additional inquiry, we will continue to investigate “French complaint 18017409.jpeg” in cooperation with our messaging service provider. At the moment, the messages indicate that the [REDACTED] has sent a STOP request to number [REDACTED] and has received a confirmation message from the messaging service provider, but based on several STOP messages sent by the client, it can be presumed that the person has not understood the purpose of the confirmation message and has incorrectly deemed it to be a marketing message.

[REDACTED] has communicated with the technical SMS platform service provider about the weaknesses of the platform. At the time of writing this letter, we have received approval from their client manager to further implement the STOP message across accounts, including to a global number.

[REDACTED] confirmed that the account of [REDACTED] has been deactivated and the non-essential personal data have been erased as of 26 August 2018. During the last inquiry of the inspection, the Inspectorate asked to be provided an estimated time when the service provider, that means the contracting partner of [REDACTED] will have resolved the processing of messages (implementation across accounts).

The Data Protection Inspectorate finds that the data controller and processor have solved the problems – a person’s account has been deleted and, in regard to the second person, the circumstances have been determined in relation to sending the STOP message. The data controller has also implemented the corresponding changes in regard to its contracting partner that means in relation to the message services.

I shall issue a reprimand to [REDACTED] in accordance with Article 58 (2) (b) of the General Data Protection Regulation and draw attention to the following:

1. When processing personal data, the data controller shall ensure that processing is lawful, fair and transparent to the data subject (Article 5 (1) (a) of the General Data Protection

Regulation). It is also important that persons are not provided with misleading information concerning the processing of personal data (including deletion of data). The outgoing messages of [REDACTED] should be clear and understandable with regard to their content.

2. The data subject shall have the right to obtain from the data controller, without undue delay, the deletion of (the account), other personal data concerning this person, and the personal data shall be subject to immediate deletion if there is no legal basis for further processing of data (Article 17 of the General Data Protection Regulation).

In view of the foregoing and the fact that the personal data of persons [REDACTED] and [REDACTED] have been deleted (the account) and the data controller has unambiguously and clearly explained the content of the sent text message, I shall terminate the supervision proceedings in this matter.

Respectfully

[REDACTED]

Senior Inspector
authorised by Director General

Summary Final Decision Art 60

Complaint

Infringement of the GDPR

EDPBI:EE:OSS:D:2019:55

Background information

Date of final decision:	7 October 2019
LSA:	EE
CSAs:	DE-Lower Saxony, DE-Rhineland-Palatinate, ES, FI, FR, LV, SK
Legal Reference:	Right to object (Article 21), Right to erasure (Article 17)
Decision:	Infringement of the GDPR, issue of reprimand in accordance with Article 58(2)(b) GDPR
Key words:	Right to object, Right to erasure, Unsolicited communication

Summary of the Decision

Origin of the case

The first complainant alleged that his right to erasure of his account and personal data had not been respected by the controller. The second complainant alleged that he could not unsubscribe from the controller's marketing text messages.

Findings

The controller carried-out an internal investigation. It became clear that, due to technical reasons, the data subject's request to unsubscribe from the text messages had not been correctly registered with the controller. Additionally, the confirmation messages sent after the second complainant's request for un-subscription from the text messages were falsely understood by the data subject to be marketing messages. Following the investigation, the controller confirmed that the first complainant's account and personal data had been deleted, and that improvements had been introduced to the text messages system.

Decision

The LSA found that Article 5 and Article 17 GDPR had been infringed, and issued a reprimand to the controller. The LSA ordered that in accordance to Article 5(1) (a) GDPR, the outgoing text messages of the controller should be clear and understandable as to their content. While in accordance to Article 17 GDPR, the right to erasure of personal data should be respected without undue delay and personal data should be deleted if there is no legal basis for further processing.



FINAL DECISION

SA Lithuania (State Data Protection Inspectorate)

Notice of termination of the proceedings concerning the protection of personal data

The Lithuanian data protection authority requested assistance from Estonia Data Inspectorate under Article 61 of the General Data Protection Regulation to resolve a pending complaint.

In the complaint person stated that [REDACTED] has sent them food supplements, although they have not given a written consent. The product was returned to the company, but they were still sent a bill for the supplements. The company has, according to the complaint, used personal data without consent.

Estonian Data Protection Inspectorate asked [REDACTED] to explain the situation and respond to the complainant. In the feedback, they have confirmed that the situation was solved in March-April and Lithuanian State Data Protection Inspectorate has been made known of this. Lithuanian State Data Protection Inspectorate has stated that they have not been informed. Nevertheless, as the situation has been solved, Estonian Data Protection Inspectorate will consider this case finalized and closed.

[REDACTED] has also provided information that the complainant has been participating in the customer survey, where she gave [REDACTED] permission to call to her phone number and offer their products. The permission was given on 15.01.2018 and the inspectorate has received the confirmation.

Therefore, we do not find [REDACTED] guilty of processing the complainant's data and we will terminate the supervision proceedings.

Respectfully

/signed digitally/
[REDACTED]

Senior Inspector
authorised by Director General

Summary Final Decision Art 60

Complaint

No violation

EDPBI:EE:OSS:D:2020:95

Background information

Date of final decision:	16 March 2020
LSA:	EE SA
CSAs:	LT SA
Legal Reference:	Principles relating to processing of personal data (Article 5), Lawfulness of the processing (Article 6)
Decision:	No infringement
Key words:	Consent, Legal basis, Legal bases, Lawfulness, Direct marketing.

Summary of the Decision

Origin of the case

The complainant claimed that the controller was sending to them unrequested food supplements, which the complainant returned and was still billed for. The complainant claimed therefore that the controller was processing their data without their consent.

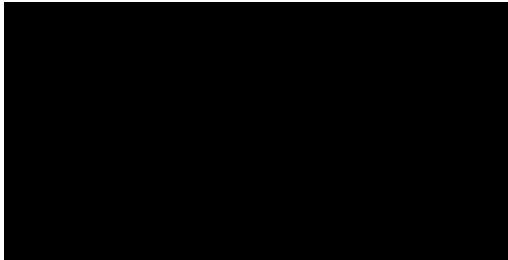
Findings

The situation had already been solved when the LSA contacted the controller. The controller also demonstrated that the complainant gave the controller permission to call to their phone number and offer their products while participating in a customer survey.

Decision

As the situation had been solved when the LSA contacted the controller and the controller demonstrated it has obtained the complainant's permission for the processing of their personal data for direct marketing purposes, the LSA considered the case finalised.

The President



Examination of the case:

Paris, on January 18th, 2019

Our Ref.: IFP/XD/DAU/CM184083

Case no. 18019404

(to be referenced in all correspondence)

Dear Mr. Director General,

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

[REDACTED] had lodged a complaint with her national data protection authority against [REDACTED] which would have not granted her request for erasure of her data recorded within the loyalty program [REDACTED]

Further to the exchanges between the CNIL and the DPO of [REDACTED] and in agreement with other European data protection authorities concerned by the processing for customer retention, I have decided to draw your attention to the breaches found during the examination of this complaint, and to reprimand you for lack of compliance with the law on the following points.

I note that the data concerning [REDACTED] have been well deleted by [REDACTED] without her having to provide any copy of an identity card since the exchanges between the latter and your services allowed to remove any doubt as to her identity.

Nonetheless, this complaint has pointed out that [REDACTED] has continued, after May 25th, 2018, to require individuals, regardless of their country or residence, to systematically provide a copy on an identity document for exercising their rights recognized by the GDPR.

I want first to outline that this practice does not, in view of its systematic nature, comply with the texts.

Admittedly, in its version prior to August 1st, 2018, Article 92 of the French Decree no. 2005-1309 implementing the Law of January 6th, 1978 required the production of such title.

RÉPUBLIQUE FRANÇAISE

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

But from May 25th, 2018, the European regulation is of direct application across all Member States of the European Union. It has in France a higher legal status than the decree no. 2005-1309.

Therefore, without waiting for the modification of this French decree, [REDACTED] should have applied the provisions of the GDPR, in particular concerning the exercise of individuals' rights, over all European territory.

Thus, throughout the exercise of the rights, it is for the data controller to ensure that the individual making the request is the data subject.

In case of reasonable doubts, he can ask to this one to prove her identity (Article 12.6 of the GDPR). Yet, such request cannot lead her to provide to the data controller more data than necessary, in application of the data minimisation principle, and the requested materials or documents have to be relevant and proportionate in light of the objective pursued.

The level of verification to be carried out is depending on the nature of the request, sensibility of the communicated information and the context within which the request is being made. For illustrative purposes, it is disproportionate to require a copy of an identity document in the event where the claimant made his request within an area where he is already authenticated. An identity document can be requested if there is a suspicion of identity theft or of account piracy for instance.

I would specifically like to draw your attention on the different national laws regulating the collection and the processing of the identification national number that is likely to appear on identity documents of data subjects.

In this context, [REDACTED] should not have requested [REDACTED] to provide a copy of an identity document as soon as she submitted her request for erasure of her data, without checking if there was a reasonable doubt as to her identity nor if this document was relevant and proportionate.

Second, I draw your attention to the fact that the data controller may in principle store the information needed for the exercise of individuals' rights, in particular documents allowing to remove a reasonable doubt, only during the period enabling to answer those requests.

Nonetheless, it can appear legitimate to store some of the data that have an interest in case of litigation during a longer period. In that case, these data have to be subject to an "*intermediary*" archiving on a support separate from the active base with a restricted access to authorized persons.

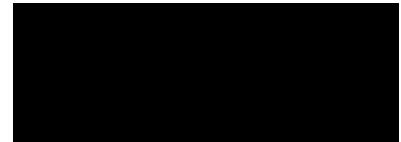
In any event, these data have to be definitely erased at the end of legal limitation applicable periods.

For more information on this point, I invite you to check the practical fact sheet entitled "*Limit data retention*" available on CNIL's website at the following URL address: <http://www.cnil.fr/fr/limiter-la-conservation-des-donnees>.

Finally, I also acknowledge that the entry into force of the GDPR on May 25th, 2018 as well as the amendments introduced in the French data protection law since June, 2018 are leading [REDACTED] SA to proceed to "*significant adaptations inside the* [REDACTED]", concerning the exercise of data subjects' rights.

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

Yours Sincerely,



Isabelle FALQUE-PIERROTIN

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

Summary Final Decision Art 60

Complaint

Reprimand to controller

Background information

Date of final decision: 18 January 2019

LSA: FR

CSAs: AT, BE, BG, CZ, DE - Bavaria (priv), DE - Lower Saxony, DE - Rhineland Palatinate, DE - Saarland, DE - Thuringia, EE, EL, ES, HR, HU, IE, IT, LT, LU, LV, NO, PL, RO, SE, SK, SI, UK

Legal Reference: Transparency and information and modalities for the exercise of the rights of the data subject (Article 12), Right to erasure (Article 17)

Decision: Reprimand to controller

Key words: Right to Erasure, Data Subject Rights not respected, proportionality for proof of identity, Reprimand

Summary of the Decision

Origin of the case

Complainant states that the right to erasure has been refused by the controller. Controller requested a scan of the ID and a specimen of the signature of the data subject. Complainant argues that neither of the two were required upon the creation of the account.

Findings

By the time of the decision, the controller had already granted the right to erasure to the complainant without the complainant needing to provide further proof of identity. However:

1. the Controller systematically requested individuals to provide a copy of an identity document for exercising their rights, regardless of their country of residence, without providing a basis for reasonable doubts as to the identity of the complainant according to Art 12.6 GDPR. "The level of verification to be carried out is depending on the nature of the request, sensibility of the communicated information and the context within which the request is being made." Thus, the controller required disproportionate information for the purpose of verifying the identity of the data subject.

The SA stated for “illustrative purposes, it is disproportionate to require a copy of an identity document in the event where the claimant made his request within an area where he is already authenticated. An identity document can be requested if there is a suspicion of identity theft or of account piracy for instance.”

2. A controller may only store information needed for the exercise of individuals’ rights until “the end of legal limitation applicable periods.” During this period, “the data have to be subject to an “intermediary” archiving on a support separate from the active base with a restricted access to authorized persons.” The LSA references <https://www.cnil.fr/fr/limiter-la-conservation-des-donnees>.

The SA highlights under “Finally”, that it acknowledges that the new data protection rules applicable are leading “to *“significant adaptations inside the”* controller, “concerning the exercise of data subjects’ rights.”

Decision

The SA reprimands “the controller for lack of compliance with the law” on the points above.