OFFICE OF
THE DATA PROTECTION OMBUDSMAN

Unofficial translation of the decision

TSV/61/2021

15.1.2025

Notice: This document is an unofficial translation of the decision of the Data Protection Ombudsman

Unofficial English translation of the decision

Case

Decision on the data subject's right to erasure in accordance with Article 60(8) of the General Data Protection Regulation

Data subject

[redacted]

Data controller

[redacted]

The applicant's claims with grounds

A case has been brought before the Office of the Data Protection Ombudsman on 24 February 2021 concerning a data subject's request to [redacted] under Article 17 of the General Data Protection Regulation (GDPR)[1] for the erasure of personal data concerning him or her.

According to the data subject, the controller has erased the user account of the data subject from the social media communications service application [redacted] provided by the controller but keeps a record that the data subject has previously used the application. The data subject has also stated in his contact on 15 November 2021 that the controller continues to process information on the data subject's age and e-mail address.

On 28 September 2023, the Office of the Data Protection Ombudsman asked the data subject whether, following the exchange of messages with the controller in January 2021, there were indications that the controller had not erased all data concerning the data subject. In its reply of 28 September 2023, the data subject has considered that the controller processes information about the data subject's e-mail address and device information which the data subject has been able to verify this by logging into the [redacted] application.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

OFFICE OF
THE DATA PROTECTION OMBUDSMAN

Background of the proceedings

The matter has previously been handled by the Office of the Data Protection Ombudsman under the registration number 1699/154/21. Due to a technical change in the system, the case has been continued under registration number TSV/61/2021.

[redacted] 's headquarters are in Berlin, Germany. Thus, pursuant to the provisions of Chapter VII of the GDPR on the handling of cross-border cases, the Office of the Data Protection Ombudsman referred the matter to the Berlin Supervisory Authority (Berlin Commissioner for Data Protection and Freedom of Information). Pursuant to Article 56 of the GDPR, the Berlin Supervisory Authority is the responsible lead supervisory authority for handling this matter.

Information received from the data controller

On 10 April 2024, the Berlin Supervisory Authority has informed the data subject of the results of the investigation carried out in the matter and the clarification provided by the data controller.

According to the information received in the case from the controller, the controller does not, in principle, process e-mail addresses of the users of the application. The identification of data subjects takes place with a pseudonymous User ID, which is created using device data when registering in the application. However, for reasons related to the system architecture of Android devices, the processing of e-mail address is necessary, but the controller does not store the data in its systems.

According to the information received from the controller, the user account of the data subject and the personal data concerning the data subject have been deleted on 8 January 2021. According to the controller, the data subject's e-mail address has been processed in connection with the customer service contact, but the information about the e-mail address has since been removed following the data subject's request on 19 January 2021. According to the controller, the controller therefore no longer processes the e-mail address of the data subject, and the controller is not able to identify the data subject. In order to identify the data subject, the controller would need information about the User ID of the data subject. In its clarification, the controller has provided instructions for finding a User ID in the [redacted] application. In addition, the controller has since changed its customer service so that, as of 29 August 2023, the processing of e-mail addresses is no longer necessary in connection with customer service.

According to the controller, if the terms of use of the platform are violated, the use of the user account may be permanently or temporarily restricted for 1-7 days. In the case of permanent blocking of the user, access will be restricted for 18 months. During this period, the following data shall be stored:

- User ID
- For iOS users
    - Pure UID
    - Device UID (hashed Pure-UID)

- For Android users
  - Advertising-ID
  - DRM-ID
- Blocked: true/false
- Reason for the ban
- Ban duration
- Information if the ban was implemented manually or automatically
- Information if the user was a moderator (having the competence to enforce the community guidelines)
- Information if the user has been banned before
- If applicable: Further details in the case
- Creator (employee of moderator) who has initiated the case

The Berlin Supervisory Authority has considered that, on the basis of the clarification provided by the controller, there are reasons to assume that the controller no longer processes the data concerning the e-mail address and age of the data subject. In addition, the Berlin Supervisory Authority considered that there was no evidence or indication in the documents submitted by the data subject that would give rise to doubts as to what had been stated in the controller's clarification.

The Berlin Supervisory Authority has stated that in order to continue the investigation, the Berlin Supervisory Authority needs to know the User ID(s) of the data subject. At the same time, the Berlin Supervisory Authority has requested the data subject to provide documentation, such as screenshots, where possible, showing that the data subject has been able to establish, through the use of the application, that the controller still processes the information concerning the data subject's e-mail address and device, or any subsequent correspondence with the data controller. The Office of the Data Protection Ombudsman forwarded the request of the Berlin Supervisory Authority to the data subject by e-mail on 10 April 2024.

The data subject's response

The data subject submitted a response in the matter on 27 April 2024. In his reply, the data subject confirmed that he had communicated all e-mail correspondence with the data controller and continued to consider that there had been an infringement of the GDPR, and that the data controller should be penalised for the infringement.

On 13 May 2024, the Office of the Data Protection Ombudsman again requested the data subject to provide information on the data subject's User IDs. The data subject did not provide the requested information.

Main elements of the draft decision submitted in the cooperation procedure

Under the cooperation procedure between the Supervisory Authorities under the GDPR, the Berlin Supervisory Authority submitted a draft decision pursuant to Article 60(3) of the GDPR on 23 September 2024.

In the draft decision, the Berlin Supervisory Authority states that, on the basis of the clarification provided by the controller, the Berlin Supervisory Authority assumes that the controller has not processed the data

concerning the e-mail address and age of the data subject since 19 January 2019. There is no evidence that the controller is still processing information on the age or e-mail address of the data subject. The draft decision states that the Berlin Supervisory Authority has examined the subject matter of the complaint to the extent appropriate. The Berlin Supervisory Authority considers that on the basis of the information provided by the data subject and the controller, it is not possible to establish an infringement of the GDPR. There is no indication that the controller will continue to process the personal data of the data subject. Furthermore, the data subject did not provide the information necessary for the continuation of the investigation. The Berlin Supervisory Authority considers that the case should not be further investigated.

As regards the device information processed as a result of the blocking of a user account, the Berlin Supervisory Authority has stated in its draft decision that, on the basis of the clarification received from the controller, the Berlin Supervisory Authority assumes that the controller has already deleted all data of the data subject, as the 18-month deletion period specified by the controller has already passed. There is no evidence to the contrary, in particular because the data subject did not provide information about his User ID, which would allow the controller to identify the data concerning the data subject. Under the prevailing circumstances, the Berlin Data Protection Authority has considered that it is not possible to find that the controller has infringed the provisions of the GDPR.

The Office of the Data Protection Ombudsman has agreed to the Lead Supervisory Authority's view on the matter.

Applicable legal provisions

According to Article 77 of the GDPR, 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.

Article 60 of the GDPR regulates cooperation between the lead supervisory authority and other supervisory authorities concerned. According to Article 60(3) of the GDPR, the lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views. According to Article 60(8) of the 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.

According to Article 78(1) of the GDPR, 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.

Under section 31, paragraph 1 of the Finnish Administrative Procedure Act (434/2003), the authority must ensure that the matter is sufficiently

and appropriately investigated by obtaining the information and clarifications necessary to resolve the case. According to section 31, paragraph 2, of the Finnish Administrative Procedure Act parties shall provide evidence of the grounds for their claims. They shall also, in other respects, cooperate in the examination of the matter which they have filed.

Article 5(1)(b) of the GDPR lays down the principle of purpose limitation, according to which personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Article 5(1)(c) of the GDPR lays down the principle of data minimisation, according to which personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

According to Article 6(1)(f) of the GDPR, the processing of personal data shall be lawful if the 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.

According to Article 6(4) of the GDPR, where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d) the possible consequences of the intended further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

According to Article 17(1) of the GDPR, the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the grounds in points (a)-(f) Article 17(1) applies.

According to Article 21(1) of the GDPR, the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the

processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Legal question

The Data Protection Ombudsman assesses and decides on the matter on the basis of the GDPR.

The Data Protection Ombudsman shall, on the basis of a draft decision submitted in the course of proceedings pursuant to Article 60 of the GDPR, approve:

1. Whether the controller has complied with the GDPR in handling the data subject's request for erasure of the data subject's Device UID pursuant to Article 17 of the GDPR.

2. Whether the controller has complied with the GDPR in handling the data subject's request for erasure of the data subject's age and e-mail address pursuant to Article 17 of the GDPR.

Decision of the Data Protection Ombudsman and its reasoning

Decision of the Data Protection Ombudsman

1. The data subject's complaint is dismissed. Based on the information received, the controller has complied with the GDPR in the handling of the erasure request.

2. The data subject' complaint is dismissed. Based on the information received, the controller has complied with the GDPR in the handling of the erasure request.

Reasoning

According to recital 141 of the GDPR the data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence, and the right to an effective judicial remedy in accordance with Article 47 of the Charter if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case.

Article 60 of the GDPR regulates the cooperation between the lead supervisory authority and other supervisory authorities concerned. The Berlin Supervisory Authority is competent to examine the data subject's complaint as the lead supervisory authority. The Office of the Data Protection Ombudsman is the supervisory authority concerned in the matter and the complaint of the data subject has been submitted to the Office of the Data Protection Ombudsman, which has referred the matter to the Berlin Supervisory Authority.

According to Article 60(8) of the 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. The Data Protection Ombudsman therefore must issue an appealable decision under Articles 60 and 78 of the GDPR.

1. Regarding the Device UID of the data subject's device

In the present case, the data subject's right to erasure of device information must be evaluated in light of points (a) and (c) of Article 17(1) of the GDPR. According to Article 17 of the GDPR, the data subject has the right to erasure. The controller shall have an obligation to erase the data without undue delay if there is a reason for erasure pursuant to Article 17(1) and if there is no exception pursuant to Article 17(3).

According to Article 17(1) the data subject shall have the right to obtain the erasure of data if the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. However, it should be noted that the data subject does not have the right to erasure on that ground if the data are subsequently processed for another purpose which is compatible with the original purpose within the meaning of Articles 5(1)(b) and 6(4) of the GDPR.

In connection with the blocking of the account, it was no longer necessary to maintain the hash-compressed value of the data subject's device UID according to the original processing purpose, which has been to provide the controller's service and use the functions of the application. However, maintaining the hash value is still necessary to ensure that blocked users do not open a new user account on their mobile device.

Taking into account the relationship between the data subject and the controller, the Data Protection Ombudsman considers that the data subject could reasonably have expected the data collected in connection with the data subject's user account to be further processed in connection with the blocking imposed on the basis of a terms of use violation. The controller has also protected the data by pseudonymisation. Therefore, the change of purpose is compatible with the original purpose.

In order for further processing to be compatible with the original purpose, it is necessary for the new purpose of processing personal data to have one of the legal grounds for processing pursuant to Article 6(1) of the GDPR. Maintaining a hash value to ensure that blocked users do not open a new user on their mobile device is a legitimate interest of the controller under Article 6(1)(f) of the GDPR. It should be noted that the procedure does not completely prevent persons who are blocked from returning to the app, but it makes it more difficult, as blocked users can re-join the app on another device. Processing a hash-condensed value for this purpose is an effective method, as the requirement to use another device generally poses an effective barrier to the creation of a new account by the same person. In addition, less restrictive means of achieving the legitimate interest pursued by the controller are not available with respect to the protection of personal data.

The Data Protection Ombudsman also notes that the interests or fundamental freedoms of the data subject, in particular the right to respect for private life and the protection of personal data[2], do not override the purpose of the processing of device information in order to restrict users who have violated the terms of use of the application, especially bearing in mind that the controller has minimised the data processed by means of pseudonymisation.

The condition relating to the necessity of the processing of personal data must also be read in conjunction with the principle of data minimisation referred to in Article 5(1)(c) of the GDPR[3]. In this respect, the assessment must take into account the controller's decision not to store the Device UID itself and to process only the hash-compressed value of the identifier by means of pseudonymisation. The procedure demonstrates that the controller has taken reasonable steps to minimise the data, limiting the personal data to be processed to those that are necessary for the above-mentioned purpose. Other options, such as saving login or contact information, would require more information about the data subject.

Moreover, an assessment under Article 17(1)(c) of the GDPR, according to which the data subject has the right to have the data erased where the data subject objects to the processing pursuant to Article 21(1) of the GDPR and there are no reasonable grounds for the processing, does not lead to a different conclusion either. The right to object to the processing of personal data must be based on a circumstance relating to the data subject's particular situation. The Data Protection Ombudsman notes that in this case, no circumstances have emerged that would require the erasure of data based on the personal situation of the data subject.

In the present case, the controller has a legitimate interest to process the data for a new processing purpose on the basis of Article 6(1)(f) of the GDPR. The processing of the hash value of the data subject's Device UID has been necessary to fulfil the legitimate interest of the controller. Furthermore, the processing of the data has been compatible with the original purpose according to Article 6(4) read in conjunction with Article 5(b) of the GDPR. The data subject does not have the right to have data concerning the data subject's device erased on the grounds set out above. The Data Protection Ombudsman therefore rejects the data subject's complaint.

Finally, the Data Protection Ombudsman notes that the information received from the controller has not revealed, nor is there any other indication that the controller still processes the data concerning the data subject's device and the blocking of the user account. According to the controller's clarification, when a [redacted] user's account is blocked, the data of the device connected to the account is stored for 18 months. In the present case, it should be noted that the data retention period defined by the controller has expired at the time of the decision in this case. Furthermore, the data subject has not provided the additional information

[2] The right to respect for private life and the right to the protection of personal data are enshrined in Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.
[3] Judgment of the Court of Justice of the European Union in Meta Platforms Inc and Others v Bundeskartellamt (4 July 2023, C-252/21), paragraph 109.

requested, which would make it possible to establish that the data would still be processed.

The data subject has not provided the authority with the information requested from him that is necessary for the continuation of the investigation in the matter. Therefore, the data subject has not contributed to the examination of the matter as required by section 31(2) of the Finnish Administrative Procedure Act.

The Data Protection Ombudsman has no reason to doubt the investigation carried out by the Berlin Supervisory Authority. The Data Protection Ombudsman agrees with the draft decision of the Berlin Supervisory Authority of 23 September 2024 and decides on the matter accordingly.

2. Processing of the data subject's e-mail address and age

According to the clarification received from the controller, the personal data of the data subject have been deleted on 8 January 2021. In addition, the controller has stated that, at the request of the data subject, on 19 January 2021, the controller deleted the personal data concerning the data subject processed in connection with the customer service contact from the controller's systems, including the data subject's e-mail address.

There is no evidence to support the claim that the controller still processes data pertaining to the age or e-mail address of the data subject. In addition, the data subject has not provided the requested information on the data subject's user IDs, which would have allowed the controller to identify the data subject.

According to the information received in the case, the controller has removed the data subject's e-mail address and age from its records in less than one month from the date of the request, as provided for in Article 12(3) of the GDPR. Based on the information received in the case, it is not possible to establish that the controller has violated the provisions of the GDPR.

The data subject has not provided the information requested from him that is necessary for the continuation of the investigation in the matter. Therefore, the data subject has not contributed to the examination of the matter as required by section 31(2) of the Finnish Administrative Procedure Act.

The Data Protection Ombudsman has no reason to doubt the investigation carried out by the Berlin Supervisory Authority. The Data Protection Ombudsman agrees with the draft decision of the Berlin Supervisory Authority of 23 September 2024 and decides on the matter accordingly.

Appeals

According to section 25 of the Data Protection Act (1050/2018), this decision may be appealed in the Administrative Court by lodging an appeal in accordance with the provisions of the Administrative Judicial Procedure Act (808/2019). Appeals shall be lodged in the Administrative Court of Eastern Finland.

OFFICE OF
THE DATA PROTECTION OMBUDSMAN

The appeal instructions are enclosed.

Service of notice

The service of notice of the decision shall be effected by post against an acknowledgement of receipt in accordance with section 60 of the Administrative Procedure Act (434/2003).

Further information on this decision is provided by the referendary

Officer [redacted]

Signature

[redacted]
Data Protection Ombudsman

[redacted]
Officer

Distribution

Data subject
Controller
The Berlin Supervisory Authority and other supervisory authorities concerned

Contact information

Office of the Data Protection Ombudsman
E-mail: tietosuoja@om.fi
Postal address: P. O. Box 800, 00531 Helsinki, Finland
Tel. (switchboard): +358 29 566 6700
Website: www.tietosuoja.fi