Berlin Commissioner
for Data Protection
and Freedom of Information

521.13790

CR: 164557

DD: 537154

FD

Berlin, 18 October 2023

Final Decision pursuant to Article 60 under the General Data Protection Regulation - [redacted]

Preliminary remarks

The complaint (ref. no. 521.13790 / 631.319) was raised before the Berlin DPA in December 2020. It was transferred to the supervisory authority in Sweden, which is the Lead Supervisory Authority (LSA) for the cross-border processing carried out by [redacted] in accordance with Article 56 GDPR. The LSA of Sweden conducted the investigation and the cooperation procedure with all concerned supervisory authorities in accordance with Article 60 GDPR. The LSA of Sweden proposed a Draft Decision and thereby the complaint was rejected. In accordance with Article 60 (8) GDPR, the Berlin DPA as the supervisory authority with which the complaint was lodged, hereby adopts the decision as it was agreed upon in the cooperation procedure and is included below:

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Alt-Moabit 59-61, 10555 Berlin
Entrance: Alt-Moabit 60

Phone: (030) 13889-0
Fax: (030) 215 50 50

Office hours: Daily from 10 am to 3 pm, Thursdays from 10 am to 6 pm

Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that the investigation of the case has not shown that [redacted] has processed the complainant's personal data in breach of Article 15 or 17 of the General Data Protection Regulation (GDPR)[1] as claimed in the complaint. The Swedish Authority for Privacy Protection dismisses the case regarding the requests submitted by the complainant to [redacted] on 31 January 2018 and 19 February 2018 from further processing. The case is closed.

Presentation of the supervisory case

Processing

The Swedish Authority for Privacy Protection (IMY) has initiated supervision against [redacted] or the company) due to a complaint. The complaint has been submitted to IMY as the lead supervisory authority under Article 56 GDPR. The handover has been made from one of the supervisory authorities of the country where the complainant lodged her complaint (Germany) in accordance with the provisions of the GDPR on cooperation in cross-border processing.
The case has been handled through written procedure. In the light of the complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Germany, Denmark, Finland, Italy, Poland and Austria.

Complaint

The complainant has mainly stated the following. On 31 January 2018, she sent a request for erasure under Article 17 of the GDPR from [REDACTED] to [redacted] replied on 5 February 2018 from [redacted] stating that the company had forwarded the complainant's case to the appropriate department which would shortly contact her.

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

On 19 February 2018, the complainant sent an email to [redacted] questioning why her request for erasure had not yet been complied with and repeated her request for erasure. [redacted] replied on 20 February 2018 and asked the complainant to send her request to [redacted] which the complainant did on the same day.

On 30 August 2018, the complainant contacted [redacted] by sending an email to [redacted] She requested access and wrote that she had repeatedly urged [redacted] to delete her personal data but that she had not received any reaction. On 12 September 2018, she sent the same email to [redacted]
On 3 October 2018, the complainant sent emails to [redacted] and to the company's customer service, repeating her requests for erasure and access. On 10 October 2018, [redacted] replied from [redacted] and asked the complainant to send her request to [redacted] The complainant replied on the same day, stating that she had already written to [redacted] but that she had not received any reaction.

What [redacted] has stated

[redacted] has mainly stated the following.
[redacted] is the data controller concerning the processing to which the complaint relates.
[redacted] received the following requests from the complainant on the below mentioned dates:

- 31 January 2018 (request for erasure)
- 19 February 2018 (request for erasure)
- 12 September 2018 (request for access and erasure)
- 3 October 2018 (request for erasure).

All requests have been handled.
[redacted] states that, in accordance with the identification requirements in force at the time of the complainant's request, the company needed to identify the customer every time a customer sent an email to the company regarding data protection issues.

Requests before the entry into force of the GDPR

Regarding two requests received on 31 January 2018 and 19 February 2018, erasure was initiated on 5 February 2018 and 22 February 2019 respectively. On 6 February 2018 and 22 February 2018 respectively, Klarna sent a confirmation to the complainant stating that erasure had been initiated. Erasure was completed on 6 February 2018 and 22 February 2018 respectively.

Request for access

Regarding the request for access received on 12 September 2018, [redacted] sent a register extract to the complainant's email address [REDACTED] on 27 September 2018, apparent from logs and an email conversation between [redacted] and the complainant annexed to the investigation. [redacted] thus complied with the complainant's request for access.
As regards the complainant's request for access in the email dated 3 October 2018, [redacted] states that, having regard to the complainant's request for access on 12 September 2018, [redacted] interpreted the latter as a reminder, or at least as part of the initial request dated 12 September 2018. During September and October 2018, the complainant sent a large number of emails to [redacted] and the interpretation that the email dated 3 October 2018 was a reminder from the complainant should be seen against this background. On 27 September 2018, [redacted] provided the complainant with a register extract and therefore does not know why the complainant sent another request for access a few days later.

Request for erasure

Regarding the request for erasure (and access) received on 12 September 2018, [redacted] asked the complainant to confirm her request for erasure, since it was not clear that Article 17 was referred to in addition to Article 15. The complainant merely mentions at the beginning of the email that she had previously contacted [redacted] regarding a request for erasure. The same year, the complainant's personal data were erased on two occasions. Since it is not clear from the request that, in addition to Article 15, the complainant also refers to Article 17, [redacted] asked for confirmation in order to: (I) inform the complainant of the consequences of erasing her data; (II) clarify the complainant's intention; and (iii) prevent the erasure of the complainant's data due to a misunderstanding as to what 'erasure of my data' means. The complainant has not confirmed

her request for erasure and [redacted] has therefore closed the case on the same day in accordance with the then existing routine and thus not complied with the complainant's request. If the complainant had replied, the case would have been reopened.
The complainant subsequently submitted several requests for erasure on 3 October 2018. As the potential erasure request received on 12 September 2018 was still marked as open when other customer service agents dealt with the request received on 3 October 2018, it seemed appropriate to consider it as part of the previously received potential erasure request. [redacted] has thus started its identification procedure as the request contained only one identification point (email address). [redacted] therefore had reasonable grounds to doubt the complainant's identity and initiated identification according to the then existing routine by requesting additional identification points.
In order to facilitate identification and thus facilitate the exercise of the complainant's rights, [redacted] referred the complainant to a previous email thread between the company and the complainant during the period from 12 to 27 September 2018 in which the complainant requested erasure and where she had already been identified. [redacted] has thus given the complainant the choice either to confirm the request for erasure in the email thread of 12 September 2018 or to be re-identified in the email thread of 3 October 2018. Since the complainant did not return to the email thread of 12 September 2018, nor to the email thread of 3 October 2018, she could not be identified according to the then existing routine. [redacted] subsequently closed the cases and did not comply with the complainant's request for erasure.

Email dated 10 October 2018

The complainant sent a request to [redacted]'s general customer service on 10 October 2018, which on the same day, in accordance with the then existing routine, referred her to [redacted]'s customer service focused on data protection issues. The case was subsequently closed. The current routine states that requests relating to data protection issues received through customer service should be forwarded by [redacted] internally to customer service focused on data protection issues after identification has been made by customer service.

Statement of reasons for the decision

Applicable provisions etc.

According to Article 99 (2) of the GDPR, the GDPR applies from 25 May 2018.
According to Article 15 of the GDPR, the data subject has the right to obtain from the controller a copy of the personal data processed by the controller. The data subject shall also receive other information, such as the purpose of the processing and to which recipients or categories of recipients the data have been or will be disclosed.
According to Article 17 (1) of the GDPR, the data subject shall have the right to obtain from the controller the erasure of his or her personal data without undue delay and the controller shall be obliged to erase personal data without undue delay if one of the conditions listed in that article exists, for example if the data are no longer necessary for the purposes for which they were collected or if consent for processing is withdrawn. Article 17 (3) lists the exceptions to this right.
The EDPB Guidelines 01/2022 on Right of access state that the GDPR does not impose any requirements on data subjects regarding the form of the request for access to the personal data. Therefore, there are, in principle, no requirements under the GDPR that the data subjects must observe when choosing a communication channel through which they enter into contact with the controller.[2] Nevertheless, if a data subject makes a request using a communication channel provided by the controller, which is different from the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle such a request accordingly. The controllers should undertake all reasonable efforts to make sure that the exercise of data subject rights is facilitated.[3]
According to the EDPB Guidelines 01/2022, the controller is not obliged to act on a request sent to a random or incorrect email (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights.[4]

The Swedish Authority for Privacy Protection's assessment

Requests before the entry into force of the GDPR

[2] EDPB Guidelines 01/2022 on data subject rights – Right of access, adopted on 28 March 2023 (EDPB guidelines 01/2022), p. 52.
[3] EDPB Guidelines 01/2022, p. 53.
[4] EDPB Guidelines 01/2022, p. 54.

According to the investigation, two of the complainant's requests for erasure were made on 31 January and 19 February 2018. [redacted] complied with those requests on 6 and 22 February 2018. The requests were thus made and handled before the GDPR became applicable on 25 May 2018.

Against this background, IMY finds that the complainant's requests of 31 January and 19 February 2018 are not covered by the GDPR and the case is therefore dismissed regarding this part from further processing.

Request for erasure and access sent to no-reply

According to the investigation, the complainant sent a request for erasure and access to [redacted] de on 30 August 2018. [redacted] provided several appropriate communication channels that could be used by data subjects to send requests to the company. For example, the complainant had previously sent requests to [redacted] and [redacted] had in an email dated 20 February 2018 asked the complainant to send her request to [redacted]

As confirmed by the EDPB guidelines 01/2022, IMY considers that the controller is not obliged to act on a request sent to a communication channel that is clearly not intended to receive requests from data subjects. Against this background, the complainant could not expect a no-reply address to be a communication channel intended to receive requests concerning the rights of data subjects. [redacted] was therefore not required to act on the request sent by the complainant to [redacted]

Against this background, IMY finds that the investigation of the case regarding this part has not shown that [redacted] has processed the complainant's personal data in breach of Article 15 or 17 of the GDPR.

Access request

According to the investigation, the complainant sent an email to [redacted] on 12 September 2018 requesting access. In a statement submitted to IMY dated 28 April 2022, [redacted] stated that the company sent an email to the complainant on 27 September 2018. The email contained, inter alia, a register extract and thus the complainant's request for access was complied with. The register extract was sent to [REDACTED], i.e. the email address used by the complainant to send her requests to [redacted] The logs and an email thread between the company

and the complainant, which [redacted] submitted during the course of the investigation, also indicate that [redacted] sent an email. Overall, IMY finds no reason regarding this part to question the company's statements.

The investigation has also shown that the complainant sent an email to [redacted] on 3 October 2018 requesting access (and erasure). She wrote the following.

"Delete my data and give me the requested access."[5]

On 27 September 2018, [redacted] had complied with the complainant's previous request for access received in September 2018. [redacted] therefore interpreted the complainant's request for access dated 3 October 2018 as a reminder of the previous request or, in any event, as part of the initial request. It was not clear to [redacted] why the complainant sent another request for access a few days later.
Given that the previous access request was complied with on 27 September 2018, the question arises whether the request for access dated 3 October 2018 should be regarded as a new request for access. The complainant's email dated 3 October 2018 does not contain any confirmation or reference indicating that she had taken note of the information sent by [redacted] on 27 September 2018. The complainant's wording in the email suggests that, for unknown reasons, the complainant had not actually accessed the copy of her personal data sent by [redacted] six days earlier. Thus, according to IMY, nothing in the email suggests that the complainant's request dated 3 October 2018 concerned a different set of personal data than covered by the request dated 12 September 2018. Furthermore, the investigation has shown that [redacted] asked the complainant on 10 October 2018 to send her request to the email address intended for data protection issues. The complainant replied the same day and wrote that she had already done so but that she had not received any reaction. IMY assesses that the complainant's reply also suggests that she intended to remind [redacted] of her initial request for access.

Against this background, IMY finds that the request dated 3 October 2018 should not be regarded as a new request for access but as a reminder of the first request dated 12 September 2018.

[5] Complaint, p. 32, IMY translation, original: "Löscht meine Daten und gebt mir meine gewünschte Auskunft".

As stated above, [redacted] replied to the complainant's request for access dated 12 September 2018 by sending an email to the complainant's email address on 27 September 2018. Subsequently, for unknown reasons, the complainant did not actually access the information. In order for the controller to be deemed to have given the data subject "access" to the personal data, it is sufficient that the data subject has been given an effective possibility to access the data. It is not necessary for the data subject to have actually accessed the data. IMY therefore finds that [redacted] fulfilled its obligations when the company sent information and a copy of the personal data to the complainant's email address.

IMY therefore considers that the complainant's access request has been handled and complied with without undue delay as stipulated in Article 12 (3) and 15 of the GDPR. Against this background, IMY finds that the investigation of the case has not shown that [redacted] has processed the complainant's personal data in breach of Article 12 (3) and 15 of the GDPR as claimed in the complaint.

Erasure request

According to the investigation, the complainant wrote in her email to [redacted] dated 12 September 2018 that in addition to her request for access she had repeatedly asked the company to erase her personal data but she had not received any reaction. [redacted] asked the complainant to confirm her request for erasure as the company considered that it was not clear that, in addition to Article 15, she had also referred to Article 17 of the GDPR. As the complainant did not reply, [redacted] closed the case.

IMY reviewed the complainant's email containing a lengthy request for access, but only one sentence stating that the complainant had previously unsuccessfully requested erasure. IMY considers that it is not clear from the request whether the complainant also intended to request erasure and that [redacted] was therefore entitled to ask the complainant to confirm whether the request should also include erasure.

According to the investigation, the complainant wrote to [redacted] and to [redacted]'s customer service on 3 October 2018 requesting (access and) erasure of her personal data. [redacted] stated that the request of 3 October 2018 was viewed as a part of the request received on 12 September 2018 as that request was still an open case. [redacted] further stated that the company

had reasonable doubts concerning the complainant's identity, since the request dated 3 October 2018 contained only one point of identification, namely the complainant's email address. [redacted] therefore initiated an identification process according to the then existing routine by requesting additional identification points in order to be able to proceed with the case. [redacted] asked the complainant either to confirm her request for erasure in the email thread of 12 September 2018, where she had already been identified, or to be re-identified in the email thread of 3 October 2018. The complainant did not reply, with the result that she could not be identified. The case was therefore closed without the complainant's request for erasure being complied with.

IMY finds that there is no reason to doubt [redacted]'s statement that the complainant did not confirm her request for erasure. IMY considers that the obligation to verify the identity of the person making a request is intended to protect data subjects against false requests made by someone else, which may lead to negative consequences for data subjects. The risks of these negative consequences in the event of false requests are particularly evident in the case of more intrusive measures, such as the exercise of the right to erasure. For a bank it is important to verify the identity of the person making a request before, for example, personal data is erased. IMY therefore considers that [redacted] was entitled to request additional identification points from the complainant in order to verify her identity.

Against this background, IMY finds that the investigation of the case has not shown that [redacted] regarding this part processed the complainant's personal data in breach of Article 17 of the GDPR.

The Berlin Commissioner for Data Protection and Freedom of Information