Swedish Authority for Privacy Protection

COMPLAINANT
See Appendices

SUBJECT OF THE SUPERVISION
iPiccolo
GDPR@ipiccolo.com

Ref no:
DI-2021-10530

Date:
2024-03-26

Decision after supervision under the GDPR- iPiccolo

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that iPiccolo AB, when handling the request for erasure made on 15 October 2018 by the complainant in complaint 1, and 13 September 2019 by the complainant in complaint 2, has processed personal data in breach of:

- Article 12(6) GDPR[1] by requesting additional information from the complainants when exercising their rights under Article 17, without the processing being necessary to confirm the identity of the complainants.

- Article 12(2) of the GDPR, by requiring, in relation to the exercise of the rights of data subjects under Article 17, that the complainants submit data in order to prove their identities by means of a special form by post. iPiccolo AB has therefore not sufficiently facilitated the exercise of the rights of the data subjects.

The Swedish Authority for Privacy Protection provides iPiccolo AB with a reprimand pursuant to Article 58(2)(b) GDPR for breach of Articles 12(6) and 12(2) GDPR.

Presentation of the supervisory case

Processing
IMY has initiated supervision of iPiccolo AB (iPiccolo or the company) in response to three complaints. The complaints have been submitted to IMY as the lead supervisory authority under Article 56 GDPR. The handover took place from the supervisory authorities of the countries where the complainants lodged their complaints (Finland and Germany) in accordance with the Regulation's provisions on cooperation in cross-border processing.

[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).

Postal address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Phone:
08-657 61 00

A decision regarding one of the complaints (submitted from Finland under national reference number 3476/182/18) is taken separately. IMY has, on the basis of the remaining two complaints, examined the company's conduct in these individual cases.

The proceedings at IMY have been carried out by exchange of letters. In view of complaints concerning cross-border processing, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The relevant supervisory authorities have been the data protection authorities of Germany, Austria, Norway, Finland, Denmark, the Netherlands, Belgium and Italy.

Complaints
The complaints in question state, in essence, the following:

Complaint 1 (Complaint from Finland with national reference number [redacted])

On 15 October 2018, the complainant submitted a request to the Finnish Data Protection Authority for erasure. The complainant replied that, in order to satisfy a request for erasure, the complainant must submit a written request with a copy of his passport or other identification document. The complainant states that company did not require the requested data previously and that, in such a case, the company would have access to more personal data than was necessary for the registration of the original customer profile.

Complaint 2 (Complaint from Germany with national reference number [redacted])

On 13 September 2019, the complainant lodged a complaint with the German Data Protection Authority. It is apparent from the complaint that the complainant has on several occasions requested the company to delete the customer account, including all personal data recorded of the complainant. The company has replied that in order to comply with the request, the complainant needs to fill in a special form, send a copy of their identity card and a third-party verification of the authenticity of the identity document.

Statement of reasons for the decision

Applicable provisions

According to Article 17(1) GDPR, the data subject shall have the right to obtain from the controller the erasure of his or her personal data without undue delay and the controller shall be obliged to erase personal data without undue delay 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 have been collected or if consent for processing is withdrawn.

According to Article 12(2) GDPR, the controller shall facilitate the exercise of the data subject's rights in accordance with Articles 15 to 22.

Article 12(6) GDPR states that, without prejudice to Article 11, where the controller has reasonable grounds to doubt the identity of the natural person submitting a request under Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The European Data Protection Board (EDPB) Guidelines 01/2022 on the right of access[2] state, inter alia, the following:

> In cases where the controller requests or is provided by the data subject with additional information necessary to confirm the identity of the data subject, the controller shall, each time, assess what information will allow it to confirm the data subject's identity and possibly ask additional questions to the requesting person or request the data subject to present some additional identification elements, if it is proportionate (see section 3.3).[3]
>
> In order to allow the data subject to provide the additional information required to identify his or her data, the controller should inform the data subject of the nature of the additional information required to allow identification. Such additional information should not be more than the information initially needed for the authentication of the data subject. In general, the fact that the controller may request additional information to assess the data subject's identity cannot lead to excessive demands and to the collection of personal data which are not relevant or necessary to strengthen the link between the individual and the personal data requested.[4]
>
> It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and, as such, it should be considered inappropriate, unless it is necessary, suitable, and in line with national law. In such cases, the controllers should have systems in place that ensure a level of security appropriate to mitigate the higher risks for the rights and freedoms of the data subject to receive such data. It is also important to note that authentication by means of an identity card does not necessarily help in the online context (e.g. with the use of pseudonyms) if the person concerned cannot contribute any other evidence, e.g. further characteristics matching to the user account.[5]

The Swedish Authority for Privacy Protection's assessment

On the basis of the complaints in question, IMY has examined the company's actions in these two individual cases.

General starting points

It can be concluded that, in order to identify a data subject, the controller may request necessary additional information if the controller has reasonable grounds to doubt the identity of the person making a request.

The GDPR does not explicitly regulate which data may be requested or how the additional information is to be collected. The controller must carry out a proportionality assessment in order to determine what is appropriate in the light of, inter alia, the requirements of the Regulation regarding security, but also in the light of the requirement in Article 12(2), according to which the controller shall facilitate the exercise of the data subject's rights. According to IMY, it is contrary to this provision to

[2] EDPB, Guidelines 01/2022 on data subject rights – Right of access, Version 2.0, adopted March 28, 2023
[3] EDPB Guidelines 01/2022, paragraph 67, translated to Swedish in official draft decision.
[4] EDPB Guidelines 01/2022, paragraph 68, translated to Swedish in official draft decision.
[5] EDPB Guidelines 01/2022, paragraph 74, translated to Swedish in official draft decision.

require information for identification without regard to the necessity of the data as described in Article 12(6).

As is apparent from the wording of those provisions and confirmed by the EDPB Guidelines 01/2022 on the right of access, the controller shall carry out a proportionality assessment and be able to justify the verification method used. Requests for additional information must be proportionate to the type of data processed and the damage that may occur in order to avoid excessive data collection.

A copy of the ID document should not be requested unless it is necessary. It is only in cases where the actual identity is of importance that it could be relevant. Identification with an ID document is not necessary if the controller has not verified the true identity of the data subject when the customer relationship was established.

In view of the requirements set out in Article 12(2), it can only be accepted in exceptional cases that a controller may refer individual data subjects to ordinary postal services as the sole means of contact when they need to submit data in order to ensure their identities, for example where this is justified for reasons of security. According to IMY, the starting point should be that alternative means of submitting the requested information should be offered.

Has there been a breach of the GDPR regarding the complaints in this case?
The question is whether the information required by the company to comply with the requests in the individual cases was necessary to identify the complainants and whether the company acted in accordance with the GDPR. The information required by the company in the individual complaints has been a signed request containing the information specified above, via a special form, and a certified copy of the ID document submitted by post.

The data subjects state that they were not offered any other option than to use regular mail when sending documents to the company. It has been an explicit requirement from the company that the requested information should be posted until 1 November 2021 when the company changed its procedures.

The company was given the opportunity to justify how each point of the personal data requested was necessary in order to identify the data subjects and why the aforementioned processing of the requests was justified in the present case. In summary, the company states that the process of filling in information by means of a form, as well as the submission of this and certified copy of the ID, by post is a process developed with the company's lawyer to ensure that no unauthorised person has access to another person's personal data. The more information the company has to search, the greater is the security that the company discloses, anonymises or deletes the right customer's personal data. Without further justification for the necessity of the respective tasks in the context of a request under Article 17, the company states that only the customer number/name and e-mail is not sufficient.

The company has stated that they have not verified the true identities of the complainants when the customer relationships were established. IMY notes that it cannot require more personal data when the complainant wishes to exercise its rights than what was required when establishing the customer relationship. Furthermore, IMY considers that according to the EDPB Guidelines on the right of access, the use of a copy of the identity document as part of the authentication process should be considered inappropriate, unless strictly necessary, appropriate and in accordance

with national law. IMY considers that the requirement to provide the controller with a copy of its identity document is an intrusive measure, which is appropriate only when the controller has previously ensured the actual identity of the data subject and where alternative less intrusive verification methods are inappropriate. IMY considers that there has been no evidence to suggest that other, less restrictive, methods of verification could have been used in the cases in question. IMY notes that it has thus not been established in the case that the request for the copy of the identity document would have been absolutely necessary or appropriate. In view of this, IMY considers that the copy of the identity document and the signature cannot therefore be considered necessary to confirm the identity of the complainants in accordance with Article 12(6) of the GDPR. Furthermore, according to IMY, the company's statement does not provide sufficient evidence to conclude that all of the other data in question were necessary to identify the data subjects in accordance with Article 12(6) of the GDPR.

Furthermore, no evidence has emerged from the investigation into the case that it could justify requiring the complainants to send the requested information to the company by regular mail or to require the complainants to use a special form to make a request for erasure. IMY therefore notes that iPiccolo AB acted in breach of Article 12(2) of the GDPR by requiring the complainants to post the data to the company when exercising the right to erasure.

Choice of intervention

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines pursuant to Article 83. Depending on the circumstances of the case, administrative fines shall be imposed in addition to or in place of the other measures referred to in Article 58(2), such as injunctions and prohibitions. In addition, it is clear from Article 83(2) which factors must be taken into account when imposing administrative fines and in determining the amount of the fine. In the case of a minor infringement, the IMY may, as stated in recital 148, instead of imposing a pecuniary penalty, issue a reprimand under Article 58(2)(b). Account must be taken of aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements.

IMY notes the following relevant circumstances. The current supervision covers iPiccolo's handling of two individual complainants' requests in the situations to which the complaints relate. The infringements found have occurred relatively far back in time and in close proximity with the entry into force of the GDPR. The Company has not previously received any corrective action for breach of the data protection regulations. In these circumstances, IMY considers that there is a minor infringement. IMY gives iPiccolo AB a reprimand pursuant to Article 58(2)(b) GDPR for the infringements found.

This draft decision has been approved by the head of unit [redacted] after presentation by the legal advisor [redacted].

Appendices: The complainants' personal data