Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision 2023-03-31, no. DI-2020-10549. Only the Swedish version of the decision is deemed authentic.

Ref no:
2020-10549,
IMI case no. 134686

Date of decision:
2023-03-31

Date of translation:
2023-03-31

Decision under the General Data Protection Regulation – CDON AB

Decision of the Swedish Authority for Privacy Protection (IMY)

The Authority for Privacy Protection (IMY) finds that CDON AB has processed personal data in breach of:

- Article 5(1)(c) and Article 12(6) of the General Data Protection Regulation (GDPR)[1] by requesting more information than necessary from the complainants in complaint 1-3 and 6-7 when they requested to have their personal data deleted without the processing being necessary to confirm their identity.

- Article 12(2) of the GDPR by using a burdensome verification method against complainants in complaint 1-3 and 6-7 without any further justification. Consequently, CDON AB did not sufficiently facilitate the complainant's exercise of their right to erasure under Article 17 of the GDPR.

The Authority for Privacy Protection issues CDON AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Articles 5(1)(c), 12(6) and 12(2) of the GDPR.

Report on the supervisory matter

The procedure

The Authority for Privacy Protection (IMY) has initiated supervision regarding CDON AB (CDON or the company) due to seven complaints. The complaints have been submitted to IMY, as responsible supervisory authority for the company's operations pursuant to Article 56 of the General Data Protection Regulation (GDPR). The handover has been made from the supervisory authority of the country where the complainants has lodged their complaints (Finland and Denmark) in accordance with the Regulation's provisions on cooperation in cross-border processing.

The investigation in the case has been carried out through correspondence. In the light of complaints relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the 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).

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

The supervisory authorities concerned have been the data protection authorities in Denmark, Norway and Finland.

Complaints

Summary of the complaints

In conclusion, the following general information can be found from the complaints. The complainants have requested the erasure of their personal data. The company has replied that a request can only be processed if the data subjects submits information about the date of birth, address, customer number, information about latest purchases such as order number and information on payment methods including the last four digits of the credit card number in case of card payment. Several of the complainants argue that their purchases were made so long time ago that they were unable to find all the information requested. The complainants dispute that all the information requested is necessary in order to confirm their identity and to handle their requests.

What the complainant and CDON have stated in the respective complaint

Complaint 1 (Finland with national registration number [redacted])

On 28 May 2018, the complainant submitted a request for the erasure of his personal data. The company has replied that a request can only be processed if the data subject submits the date of birth, address, customer number, order number, payment method for the latest order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

In conclusion, the complainant states that she cannot remember or find the information requested by the company since the order was made 5-10 years ago.

Complaint 2 (Finland with national registration number [redacted]

On 25 May 2018, the complainant contacted CDON and requested the erasure of its customer data. The company has replied that they require information on the date of birth, customer number, order number and payment method for the latest order. The complainant states that it is unreasonable to have to answer these questions in order to be able to exercise its rights. The complainant does not retain the information requested by the company and has used the e-mail linked to the customer account for the request for erasure.

Complaint 3 (Finland with national registration number [redacted])

On 31 May 2018, the complainant contacted the Finnish Data Protection Authority after requesting access to and erasure of the complainant's data at the company. On 29 May 2018, CDON replied to the complainant's request that, in order to verify the complainant as a customer they need, their address, customer number, order number from the last order, payment method for the last order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

The complainant states that it was a long time ago something was purchased from CDON and that he or she does not have the information the company requires. It is

further stated that the company does not seem to delete the data without receiving answers to its detailed questions in the event of a request for erasure.

Complaint 4 (Finland with national registration number [redacted])
On 31 May 2018, the complainant applied to the Finnish Data Protection Authority after requesting erasure from the company. It was 5-10 years ago since the complainant ordered something from CDON. In order to be able to delete their data, the complainant needs to send data from his purchase that is from several years back in time to the company. The complainant also needs to provide personal data that was not previously needed to make a purchase in the first place. The company informed in its reply to the complainant that there is a right to access and erasure of personal data but that the company as a controller has the right to retain certain personal data for accounting purposes. In order to comply with a request, for security reasons, the company needs to be informed of the complainant's date of birth, address, customer number, order number from the last order, payment method for the latest order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

The company states that it is not in a position to verify the date on which the complaint was lodged with the company or the date on which it requested additional information from the complainant. Since the complainant have not been active customer of CDON for the last two to five years, CDON also confirms that the complainants' personal data were removed from CDON's system and that no information on the complainant remains.

Complaint 5 (Finland with national registration number [redacted])
The complainant has contacted the Finnish Data Protection Authority after requesting the erasure of its data at the company. The company have informed the complainant that there is a right to access and erasure of personal data but that the company has the right to retain certain personal data for accounting purposes. In order to comply with a request, for security reasons, the company needs to be informed of the complainant's date of birth, address, customer number, order number from the last order, payment method for the latest order:

- If invoice: price and reference number
- If card payment: the last four digits of the credit card number
- If direct payment: reference number and receipt

The complainant does not remember when an order was placed from the company and how the purchase was paid. It's been over a year since something was ordered.

The company states that it is not in a position to verify the date on which the complaint was lodged with the company or the date on which it requested additional information from the complainant. Since the complainant have not been active customers of CDON for the last two to five years, CDON also confirms that the complainants' personal data were removed from CDON's system and that no information on the complainant remains.

Complaint 6 (Finland with national registration number [redacted])
The complainant lodged a complaint with the Finnish Data Protection Authority following a request for erasure from the company on 21 May 2018. The complainant

states that the company makes it difficult to exercise the right to erasure by requesting information that a customer should not be obligated to save. The process contributes to a long wait until the request of right to erasure is met. In its reply to the complainant on 29 May 2018, the company requested information on the date of birth, address, customer number and one of the following:

- Order number from the last order;
- Payment method for the last order:
- if invoice: price and reference number
- if card payment: the last four digits of the credit card number
- if direct payment: reference number and receipt

Complaint 7 (Denmark with national registration number [redacted])
The complainant claims to have attempted to delete his customer account online on cdon.dk by using a hyperlink http://cdon.dk/. The company replied to the complainant on 29 May 2018 requesting information regarding the date of birth, address, customer number, order number from the last order, payment method for the last order including the last four digits of the credit card number. The complainant states, inter alia, that the company requires more information when exercising the right to erasure than in the creation of the customer account. The complainant used the same e-mail address for the request for erasure as for the creation of a customer account at the company.

What CDON AB has stated

CDON AB has mainly stated the following.

Complaints
Of the complaints covered by this case, CDON has been able to identify six out of seven complainants against information in its systems. As regards to those six complainants, CDON is the controller of the processing of personal data to which the complaints relate.[2]

When the company received the requests for erasure, it contained the complainants' name and e-mail address. However, CDON considers that only those two data are not sufficient to ensure the identity of the complainant. CDON has therefore requested additional information from all complainants pursuant to Article 12(6). In addition to their name and e-mail address, the complainants were required to provide the following information in order to ensure their identity:

- Date of birth;
- Address of civil status;
- Customer number;
- The order number of the latest order; and
- Payment method for last order.

In addition, the complainants had to provide the following information on payment methods:

- In the case of invoice purchases: price and reference number;
- In case of card payment: the last four digits of the card;
- In case of direct payment: reference or invoice number.

[2] CDON has not been able to identify complainant in complaint [redacted] (complaint 5). However the company has stated that it is possible that the complainant has had a customer relationship with CDON under a different email address than indicated in the complaints sent to the supervisory authority which cannot be verified.

Current routine
In this context, CDON deems, receiving complaints concerning difficulties for data subjects in exercising their rights under the GDPR to be a matter of concern and has therefore continuously worked to improve its identification procedures when exercising the right of erasure and access. Since 2018, when the complaints were received, the identification process has been reviewed and clarified. Over the years, CDON has worked to improve handling and ensuring a simple and secure process for requests for erasure. Customers who wish to request erasure or access are directed to contact the customer service at kunddata@cdon.com. When a data subject contacts the company with a request for erasure, the company informs the data subject that the data subject's e-mail will shortly be unsubscribed from the CDON newsletter (if such subscription is activated). In order to have their account deleted, CDON currently asks the customer to answer two security questions (one each from category 1 and 2) in order for CDON to ensure that the person who contacted the company is correctly registered. Data subjects may choose to answer one question from the respective security category of questions provided by CDON. This means that data subjects need to answer only one of the following category 1 security questions. According to the verification questions in category 1, customers must state the date of birth[3], the registered address or the customer number on CDON.com. Thereafter, data subjects need to answer only one of the following category 2 security questions. The control questions in category 2 are connected to recent orders where the customer either enters the order number or, depending on the payment method, enters one of the following information: when invoiced; amount and OCR number, in case of card payment: the last four digits on the card and in the case of direct payment; transaction ID or invoice ID.

In the event that a customer does not want or is unable to answer the security questions requested, the data subject is also offered the opportunity to contact customer service to follow-up and investigate an alternative security method to verify the data subject's identity. CDON considers it necessary to provide at least two additional information in addition to the name and email address of customers according to the company's new routine in order to be able to verify with sufficient certainty that it is the right person making a request. CDON's procedure for the identification and verification of the data subject does not involve the collection of new information about the data subject. CDON only requests to have two different data verified against the data that CDON already processes about the data subject with a legal basis in order to verify the identity of the data subject.

The company's retention period
CDON has stated that they have a separate retention period for e-mail and another retention period for personal data. CDON's retention period for e-mail means that all emails received to CDON's customer data box i.e. kunddata@cdon.com to which customers are referred to if they have requests for erasure or access, will be deleted after 14 months from the date of receival at CDON. The erasure of customer profiles on CDON is currently carried out based on consumer law obligations in different countries, for example after three years in Sweden. CDON therefore confirms that all complainants have been deleted at CDON.

[3] Since 22 January 2021, CDON only collects birth numbers (if data subjects choose to add that information in category 1) and not the full personal identity number.

Justification of the decision

Applicable provisions, etc.

In order for personal data processing to comply with the GDPR, the processing must inter alia comply with the requirements regarding the principles of processing of personal data set out in Article 5 of the GDPR, including the principle of data minimisation (Article 5(1)(c) and the principle of accountability (Article 5(2).

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

According to Article 11(2) where in the cases referred to in paragraph 1 of this article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling the identification.

Article 12(2) requires the controller to facilitate the exercise of the data subject's 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.

Article 12(6) provides that, without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred in 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 state as follows.

As indicated above, if the controller has reasonable grounds for doubting the identity of the requesting person, it may request additional information to confirm the data subject's identity. However, the controller must at the same time ensure that it does not collect more personal data than is necessary to enable authentication of the requesting person. Therefore, the controller shall carry out a proportionality assessment, which must take into account the type of personal data being processed (e.g. special categories of data or not), the nature of the request, the context within which the request is being made, as well as any damage that could result from improper disclosure. When assessing proportionality, it should be remembered to avoid excessive data collection while ensuring an adequate level of processing security.[4]

The controller should implement an authentication procedure in order to be certain of the identity of the persons requesting access to their data, and ensure security of the processing throughout the process of handling an access requests in accordance with Art. 32 GDPR, including for instance a secure channel for the data subjects to provide additional information. The method used for authentication should be relevant, appropriate, proportionate and respect the data minimisation principle. If the controller

[4] EDPB Guidelines 01/2022 on data subject rights - Right of access Version 2.0 Adopted on 28 March 2023, paragraph 70.

imposes measures aimed at authentifying the data subject which are burdensome, it needs to adequately justify this and ensure compliance with all fundamental principles, including data minimisation and the obligation to facilitate the exercise of data subjects' rights (Art. 12(2) GDPR).[5]

Assessment of the Authority for Privacy Protection (IMY)

Complaints
Pursuant to Article 57(1)(f) of the GDPR, IMY shall deal with complaints and, where appropriate, investigate the subject matter of the complaint. The case includes seven complaints. IMY has requested CDON to comment on the information it has requested, the need for each individual information, the date on which the request for erasure was received in the respective complaints, the date on which it requested additional information to confirm the identity of the respective complaints and whether the complainant contacted the company after 25 May 2018.

Complaints 4 (Finland with national registration number [redacted]) and 5 (Finland with national registration number [redacted]) do not indicate the date on which the complainant made a request for erasure with the company or when the company requested the additional information. The company has stated that it has deleted the complainant's personal data in these two individual complaints in accordance with its retention period procedure and cannot verify the date on which the request in the respective complaint was received or handled. IMY finds no reason to doubt that CDON was unable to find any information about the complainant and its request for erasure. Several years have passed since the complaints were submitted to the Finnish Data Protection Authority.

IMY notes that it is not possible to draw any conclusive conclusions from what has been done in the two complainants' case on the basis of what has been possible to investigate in the complaints. In particular, in view of the fact that the complainants' requests relate to the time close to when the GDPR entered into force, it has not been possible to ascertain whether those two complaints fall within the scope of the GDPR. CDON has further confirmed that no personal data relating to these two complainants are no longer being processed by the company. Against this background, IMY considers that the substance of the complaint is investigated to the extent appropriate under Article 57(1)(f) of the GDPR. IMY therefore finds no reason to investigate these two complaints further.

Consequently, IMY has, on the basis of the remaining five complaints in the case, examined the company's conduct in these individual cases. IMY has also examined whether the company's current routine is compatible with the General Data Protection Regulation.

General starting points

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

[5] EDPB, Guidelines 01/2022, paragraph 71.

The GDPR does not explicitly regulate what 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 with regard to the Regulation's requirements, inter alia, for security reason, but also in the light of the requirement in Article 12(2) of the GDPR, according to which the controller shall facilitate the exercise of the data subject's rights. IMY finds that, requiring data on general basis for identification purposes irrespective of whether the data is necessary as described in Article 12(6) is contrary to both this provision and also to the principle of data minimisation in Article 5(1)(c).

As follows from the wording of the above-mentioned provisions which is also confirmed by the EDPB Guidelines 01/2022 on the right of access, the controller must carry out a proportionality assessment and be able to justify the verification method used. In order to avoid excessive data collection, a request for additional information must be proportionate to the type of data being processed and the damage that it may occur. This is also confirmed by the guidelines.[6]

Has there been an infringement of the GDPR in regards to what has been raised in the complaints in this case?

The question is whether the information required by the company to comply with the requests in the individual cases where the GDPR applies (i.e. complaints 1-3 and 6-7) has been necessary to identify the respective complainant and thus in accordance with the GDPR. The information that the company has required, in addition to name and e-mail, has been the date of birth, the civil registration address, customer number, order number and payment method for the latest order, and, depending on the payment method, price and reference number for invoice payment, the card's last four digits for card payment or reference or invoice number in case of direct payment.

The company has been given the opportunity to justify if all of the required personal data requested was necessary in order to identify the complaints in the individual cases. Without further explaining the necessity of the information requested, the company has stated to IMY that it was not enough with only name and e-mail to identify the complaints and verify that it was the correct person making the request. IMY finds that, the company's statement does not provide sufficient evidence to conclude that all of the requested data at issue were necessary to identify the data subjects in accordance with Article 12(6) and the principle of data minimisation in Article 5(1)(c). As a data controller CDON shall be able to demonstrate that the processing is carried out in accordance with the GDPR (Article 5(2)). IMY believes that CDON has not done so. IMY therefore notes that CDON AB processed personal data in breach of Article 5(1)(c) and 12(6) of the General Data Protection Regulation.

In the present case, the complainants had to provide a relatively large number of personal data in order to exercise their right to erasure, including the order number and the price of the latest order and the reference number for invoice purchases together with additional information. In some cases, it has been a long time since the complainants has purchased anything on CDON. This means that the complainants have not been able to exercise their right to erasure under Article 17 without having to make an effort to search for a large amount of information and in some cases also information that is quite old. Thus, by using such a burdensome verification method in the handling of request for erasure without justification, the company has not facilitated

[6] EDPB, Guidelines 01/2022, General considerations on the assessment of the data subject's request, page 2-3.

the exercise of data subjects' rights as required by Article 12(2). CDON AB has thus processed personal data in breach of Article 12(2) of the GDPR.

Is the company's current routine compatible with the GDPR?

The investigation shows that the company has continuously reviewed its procedures for handling requests for erasure since 2018, when all the complaints in the case were received. The general routine examined are those in force from 22 January 2021 until the date of IMY's decision in the case in question.

In order to ensure the identity of the data subject requesting erasure, the data subject now needs to answer two questions (one question in category 1 and one question in category 2) such as date of birth and order number. Since 22 January 2021 the data subjects does not need to provide a personal identity number but only the date of birth if the data subject chooses to add that information in category 1. It is not new personal data that is requested to confirm the identity of the data subject, but two different data to compare it with data that the company already is processing regarding the data subject in order to verify the data subject. The fact that CDON verifies the identity of the data subject before erasure of personal data is also a protection for the data subject who should not have his or her personal data deleted by mistake. The company also offers an alternative way for the data subject who cannot or does not want to answer the security questions, namely to contact the customer service to find another way to verify the identity of the data subject. Therefore, a customer who has not placed an order, there is the option to contact customer service instead.

Against this background, IMY considers that CDON's existing routine is not disproportionate and therefore not in breach of the GDPR, provided that it collects only the data contained in the routine in situations where there is reason to doubt the identity of the data subject and that only the data necessary to identify the data subject is requested.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has the power to impose administrative fines in accordance with 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. Furthermore, Article 83(2) provides which factors are to be taken into account when deciding on administrative fines and in determining the amount of the fine. In the case of a minor infringement, as stated in recital 148, IMY may, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Factors to consider is the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and past relevant infringements.

IMY notes the following relevant facts. The investigation in question covers CDON AB's handling of five individual complainants' requests in relation to the respective complaints.

The company has taken measures to make it easier for data subjects to exercise their rights in accordance with the GDPR and changed their procedures to ensure that they are compliant with the GDPR. Some measures had already been taken before the start of this supervisory case. Furthermore, the infringements found occurred relatively

long time ago. In addition, the company has not previously acted in breach of the GDPR.

Against this background, IMY considers that this is a minor infringement within the meaning of recital 148 and that CDON AB must be given a reprimand in accordance with Article 58(2)(b) of the GDPR for the infringements found.

This decision has been made by [redacted], Head of Unit, after presentation by legal advisor [redacted].

How to appeal

If you want to appeal the decision, you should write to the Authority for Privacy Protection. Indicate in the letter which decision you appeal and the change you request. The appeal must have been received by the Authority for Privacy Protection no later than three weeks from the day you received the decision. If the appeal has been received at the right time, the Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to the Authority for Privacy Protection if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. The authority’s contact information is shown in the first page of the decision.