Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's decision.

COMPLAINANT
See appendix

DATA CONTROLLER
Ellos Group AB

Registration number:
DI-2021-5451

Case register/National registration number:
CR 155123
4098/182/2018,
801/163/2019

Date:
2024-09-03

Decision under the General Data Protection Regulation– Ellos Group AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection finds that Ellos Group AB (org. nr. 556217-1925) has processed the complainant's personal data in any event during the period from 6 July 2018 to 30 June 2021 in breach of Article 32 of the GDPR[1] by failing to take appropriate technical and organisational measures to ensure adequate protection against unauthorised disclosure on its website of personal data in the complainant's customer profile.

The Swedish Authority for Privacy Protection issues a reprimand to Ellos Group AB pursuant to Article 58(2)(b) of the GDPR for breach of Article 32 of the General Data Protection Regulation.

Presentation of the supervisory case

Handling of the case

The Swedish Authority for Privacy Protection (IMY) has initiated a supervision regarding Ellos Group AB (Ellos) due to two complaints. The complaints have been submitted to IMY, as lead supervisory authority under Article 56 GDPR. The handover has been made from the supervisory authority of the country where the complainants has lodged their complaints (Finland) 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 concerning a cross border processing, IMY has used the mechanisms for cooperation

[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, Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
08-657 61 00

and consistency contained in chapter VII of the GDPR. The supervisory authorities concerned have been the Finnish Authority for Privacy Protection.

The complaints

The complainant has mainly stated the following. The complaints allege a security flaw on the websites of Ellos, Ellos and Jotex online store (ellos.fi and jotex.fi). The complainants have observed that it was possible for them to log in to the Ellos online store using only email and postcode. Thus, no password or other verification method was needed for login. After the complainants have logged in with the new method, you can see the individual's profile including; telephone number and address and the nearest delivery point. Even if the address is partly hidden, it is not difficult to guess the correct address with the help of the nearest delivery point. One of the complaints also states that it is possible to see the individual's purchase history.

What Ellos has stated

Ellos Group AB has mainly stated the following.

Ellos is the controller of the processing operations to which the complaint relates.

The login method to which the complaints relate is referred to as ‘soft log-in’. It is a simplified login to Ellos and Jotex online stores that allows the customer to access certain features of the online store. The simplified login is a common solution in the industry with the aim of providing benefits to already registered customers by facilitating their purchase process.

Through soft log-in it is possible to place orders for products in the online store. At the checkout, the customer can see their pseudonymised information about their name, address and telephone number, as well as information about possible delivery points. Pseudonymisation means that the data can only be identified by someone who already has knowledge of the complete data. In addition to this, no access to purchase history and other customer data is given at soft log-in. Access to purchase history and other customer information requires the customer to make a full login with password.

Before placing an order, there is a clear request to the customer to ensure that the pseudonymised personal data displayed is correct. If the personal data is incorrect, there is a reference where the customer can log in to their customer account with a full login. When ordering, a confirmation email always goes to the email address registered in the account, so that the account holder has the opportunity to cancel the order if it has been made by the wrong person. Delivery can only be made to the address registered in the customer account or a delivery point. If delivery is made to a delivery point, the product cannot be collected without the registered customer's ID document. The customer always has the right of withdrawal if someone else has placed the order in the customer's name.

In summary, there are a number of security measures built into the soft log-in process to prevent the wrong person from placing an order in the name of another customer, as well as to prevent an order from being placed by the wrong person. The risk that unauthorized use of someone else's customer account when ordering is completed to the detriment of the customer is thus limited. Overall, the requirement for appropriate security measures under the General Data Protection Regulation is met.

When asked how Ellos ensured, in relation to the complainants in the complaints, that the right persons had access to the data and ordered products when ordering over the internet, Ellos replied as follows.

As mentioned above, before placing an order, the complainants have been clearly instructed to ensure the accuracy of the pseudonymised personal data displayed. It is not apparent from the complaints that the complainants ordered any products. Ellos works continuously to review and evaluate its work processes and security measures to protect data subjects' personal data and to promote a safe customer experience on the internet.

Statement of reasons for the decision

Applicable provisions

Article 32 of the GDPR governs the security of processing. The controller shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons, take appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In assessing the appropriate level of security, particular account shall be taken of the risks posed by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Assessment of IMY

The investigation in the case shows that Ellos uses a so-called ‘soft log-in’. This is a login method that only requires the customer to provide their email address and postal code in order to access a part of their customer profile. The ‘soft log-in’ mode shows the customer’s name, address, telephone number and the nearest delivery point. One of the complaints states that the customer's purchase history is also shown, but this is disputed by Ellos. There is no support in the investigation to question Ello’s statements that purchase history is not shown after the ‘soft log-in’.

When processing personal data, they shall be processed in a way that ensures appropriate security of the personal data based, inter alia, on their sensitivity. Personal data such as name, telephone number and address data are not sensitive data under Article 9 of the General Data Protection Regulation, nor are they particularly worthy of protection, such as personal identity numbers, nor so-called privacy-sensitive data. Current categories of data exist in some Member States in publicly available sources (including in Sweden with the exception of so-called protected personal data and in Finland with the possibility to request a ban on the disclosure of personal data).

Exposure of personal data on the internet is a particular risk in itself when the data is made available to an unlimited number of natural persons. The current risk is that people who do not want their data to be disseminated openly on the internet will still have their personal data exposed.

When processing personal data, they shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or

unlawful processing.[2] Authentication means that users confirm their declared identity. It is about ensuring that the right user has access to a user account or system. Authentication can be done by the user entering their username and password in order to access a program, service or system.

Authentication is a two-step security measure. First, the user *identifies* themselves and then the user *verifies* the declared identity with some form of authentication tool, such as a password. In the described ‘soft log-in’ process, users identify themselves with their email address. However, no actual verification is carried out, as postal codes are publicly available information that can be accessed via, for example, the Finnish Post Office's website (posti.fi). Postal codes can be linked to an individual and are neither ‘secret’ nor individual. The personal data contained in the ‘soft log-in’ customer profiles therefore lack authentication protection. The lack of protection means that people who do not want their data to be disseminated openly on the internet still risk having their personal data exposed.

Ellos has stated that the personal data on the website is psedonymised. Pseudonymisation is a security measure whereby personal data are processed in such a way that the personal data can no longer be directly attributed to a specific data subject without the use of additional data, provided that such additional data are kept separately and are subject to technical and organisational measures that ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymised personal data is still personal data, although the risk of identifying a person is reduced, as the possibility of identification still exists. From what has emerged from the complaints, the processing of personal data on Ellos website means that the address information is only partially hidden. It is possible with the help of the nearest delivery point, which is also shown on the website, to find the right address. Thus, additional data enabling the personal data to be attributed to a specific data subject are not kept separately. IMY therefore considers that the measure known as the psedonymisation of Ellos is not such as to achieve an appropriate level of security in relation to the risk of the appellants’ personal data being exposed via the internet.

IMY considers that the appellants’ personal data have been exposed via the internet without adequate protection and, therefore, that the data have been made accessible to an unlimited number of natural persons. IMY notes that the measures taken by Ellos did not sufficiently reduce the exposure of the complainants’ personal data via the internet. It has thus not provided an appropriate level of security in relation to the risks posed by processing.

In conclusion, IMY finds that Ellos has not taken appropriate technical and organisational measures under Article 32 to ensure adequate protection against unauthorised disclosure on its website of personal data in the complainant’s customer profile. Ellos has thus processed personal data in breach of Article 32 of the GDPR.

Choice of corrective measure

It follows from Article 58(2)(i) and Article 83(2) of the GDPR that 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 instead of the other measures referred to in Article 58(2), such as reprimand, injunctions and prohibitions. Furthermore, it is clear from Article 83(2) which factors

[2] Article 5(1)(f) GDPR

must be taken into account when deciding on an administrative fine and when determining the amount of the fine. Account needs to be taken to the aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement as well as past infringements of relevance.

IMY notes the following relevant facts. The current supervision covers Ellos processing of complainants' personal data in the situation to which the complaint relates. The infringement was not intentional but negligent. Against that background, IMY considers that that infringement is not of such a nature that a fine should be imposed and that Ellos Group AB shall therefore be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

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

The IT and information security specialist [redacted] was also involved in the final processing of the case.

Appendix
The complainant’s personal data 1
The complainant’s personal data 2

Copy to:
The company’s DPO

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.