Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) final decision 2022-03-29, no. DI-2021-4664. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-4664, IMI case no. 134632

Date of final decision:
2022-03-29

Date of translation:
2022-03-31

Supervision under the General Data Protection Regulation – Ellos Group AB

Final decision of the Swedish Authority for Privacy Protection (IMY)

The Swedish Authority for Privacy Protection (IMY) finds that Ellos Group AB has processed personal data in breach of Article 32(1) of the General Data Protection Regulation (GDPR)[1] by failing to take appropriate technical and organizational measures until 21 May 2021 to ensure an appropriate level of security for the company's "merge customer" process.[2]

The Authority for Privacy Protection issues Ellos Group AB a reprimand pursuant to Article 58(2)(b) of the GDPR for the infringement of Article 32(1) of the GDPR.

Report on the supervisory report

The Authority for Privacy Protection (IMY) has initiated supervision regarding Ellos Group AB (Ellos or the company) due to a complaint. The complaint has 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 complainant has lodged their complaint (Norway) 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 a complaint relating to cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII GDPR. The supervisory authorities concerned have been the data protection authorities in Norway, Denmark and Finland.

Postal address:
Box 8114
104 20 Stockholm

Website:
www.imy.se

E-mail:
imy@imy.se

Phone:
08-657 61 00

[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 he processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
[2] The "Merge customer" process means hat two or more accounts on a website can be merged into one, in case a person establishes several accounts with the same personal data.

The complaint
It is stated in the complaint that the complainant wished to assist their cousin in receiving an order from Ellos. The cousin therefore used the complainant's postal address when placing the order. A few days later, when the complainant tried to log into their Ellos account, the account was deleted or blocked. The complainant's cousin was then able to access, through their account, the complainant's purchase history. The complainant has been in contact with the company's customer service but has not had the problem solved. The complainant considers that there is a lack of safety. The complainant also states that they could have had their credit card details registered in their customer account, which they did not have.

What Ellos has stated
Ellos has mainly stated the following.

Ellos is the data controller for the processing to which the complaint relates.

The company has a process called "merge customer" which means that when a new customer profile is created and the new profile consists of identical data already registered in an existing customer profile, the existing customer profile is merged with the new one. In creating an account, the complainant's cousin used the complainant's first name, surname, street name, street number and postcode. The complainant's customer profile was then merged with the new customer profile created by the complainant's cousin.

According to the company, the purpose of the "merge customer" process is to merge user accounts if there is reason to assume that a customer does not remember their login details and therefore registers again. This is done in order to limit the processing of personal data by the company to updated and current data. The process was introduced as a more privacy-friendly option when the GDPR entered into force, in order not to use social security numbers as an identifier.

When the accounts of the complainant and their cousin were merged and the cousin tried to place an order from the new account, an e-mail was sent to the previously registered e-mail address, i.e. the complainant's e-mail, so that the ordering process could be interrupted if the wrong person had attempted to place the order. When the complainant contacted Ellos and stated that the order was placed by someone else (the cousin), the account was temporarily blocked.

At the time when the "merge customer" process took place, the complainant's cousin did get access to the complainant's purchase and return history. However, the cousin did not have access to invoices, payment card details or other information on payments.

Ellos states that, after receiving IMY's inspection letter, it has taken steps to ensure that the purchase history is not available in case the "merge customer process" is activated. Ellos further states that it is working on implementing corresponding security measures regarding access to the return history. According to the company, the implementation is expected to be completed in the near future.

The company also states that they intend to contact the complainant in order to provide information on how the complainant can lift the block on its account.

Justification of the decision

Applicable provisions, etc.

Any processing of personal data must comply with the fundamental principles set out in Article 5 of the GDPR. One of these is the requirement of security under Article 5(1)(f). It follows that personal data must be processed in such a way as to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 32 regulates the security of processing. Paragraph 1 requires the controller, taking into account the latest developments, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, of varying probability and severity, to the rights and freedoms of natural persons, to take appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

According to Article 32(2), when assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by 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 the Authority for Privacy Protection (IMY)

Has the company infringed Article 32(1) of the General Data Protection Regulation?

IMY notes, first of all, that Ellos Group AB, after the supervision started on 21 May 2021, has taken steps to ensure that the purchase history is not available upon activation of the “merge customer process” and intends to take measures to ensure that the return history is not available. The investigation has not shown that there is reason for IMY to question the use of the “merge customer” process based on the company’s purpose of limiting the company’s processing to current and updated personal data, after the abovementioned improvements have been made.

However, IMY has found that the “merge customer process” prior to the start of supervision on 21 May 2021 was designed in such a way that a customer’s purchase and return history could be made available to unauthorised persons by creating a new account with an existing customer’s first name, surname, street name, street code and postal code. Since the information required to create a new account was publicly available in open sources, for example in online directory services, information on customers’ buying habits has not been sufficiently protected against unauthorised disclosure. According to IMY’s assessment, the deficiency should have been detected at an early stage prior to the start of the processing of personal data. Ellos Group AB has thus processed personal data in breach of Article 32(1) of the GDPR.

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 company has taken measures to protect information about customers' buying habits from unauthorised disclosure. Neither sensitive nor integrity-sensitive data has been involved. The infringement was committed negligently, affected one person and, when the company understood the complainant's intention, it took action. IMY has not previously established that the company has infringed the GDPR.

Against this background IMY considers that it is a minor infringement within the meaning of recital 148 and that Ellos Group AB must be given a reprimand pursuant to Article 58(2)(b) of the GDPR.

This final decision has been made by the specially appointed decision-maker [redacted] 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.