COMPLAINANT
See appendix

CONTROLLER
Care of Carl AB

Swedish ref.:
IMY-2025-684

FI SA ref.:
TSV/9948/2024

IMI case register:
724772

Date:
2026-06-18

Final decision pursuant to Article 60 under the General Data Protection Regulation – Care of Carl AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Care of Carl AB (org no 556800-5739) has processed the personal data of the complainant in breach of Article 32 of the General Data Protection Regulation (GDPR)[1] by failing to implement sufficient measures to ensure an appropriate level of security of the complainant's personal data during the processing in question.

IMY issues a reprimand to Care of Carl AB pursuant to Article 58(2)(b) of the GDPR for the infringement.

Presentation of the supervisory case

IMY has initiated supervision regarding Care of Carl AB (the company) in order to investigate whether the processing of the complainant's personal data in the function of automatic filling of data meets the requirements for security under Article 32 of the GDPR. The complaint has been submitted to IMY, as lead supervisory authority pursuant to Article 56 of the GDPR. The handover has been made from the supervisory authority of the country where the complaint has been lodged (Finland) in accordance with the provisions of the GDPR on cooperation in cross-border processing.

The case has been handled through written procedure. In 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 concerned supervisory authorities have been the data protection authorities in Finland, the Netherlands, Austria, Italy, France, Norway, Denmark, Spain and Germany.

Postal address:
Box 8114
104 20 Stockholm
Sweden

Website:
www.imy.se

E-mail:
imy@imy.se

Telephone:
+46 (8) 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 the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Complainant

The complainant has essentially stated the following. When the complainant entered his postal code and e-mail address at Checkout on the company's website, the rest of the data was filled in automatically. This occurs even when the complainant wasn't logged in, searched in Incognito mode and used a VPN. The same automatic filling occurs even on different devices. It is not possible to decline the function. Even though the data which is automatically filled is partially masked with asterisks, it is possible to figure out the data. It is thus possible to test different combinations of email addresses and postal codes until a match is found. This is a significant security risk.

The company

The company has essentially stated the following. The processing of personal data to which the complaint relates meets the requirements for security measures under the GDPR. The personal data processed in the situation in question consists of basic contact and delivery data and the processing is done in order to facilitate for existing customers when purchasing. Based on an overall risk analysis, the likelihood of actual injury to the data subject is considered to be limited. Nonetheless, technical and organisational measures have been taken to prevent unauthorised access, systematic testing and improper mapping of personal data.

The company has taken the following technical security measures in the in-house developed check-out:

- The company has a server-based masking in the checkout interface, i.e. name and address details are presented only partially masked in the checkout flow. The masking takes place on the server side, which means that the complete data is not exposed in the client and cannot be accessed or recreated via the user interface.
- Full personal data is stored in an encrypted database, with limited access and controlled by access controls.
- The autofill feature is only available within the checkout flow and cannot be accessed via external or public interfaces or APIs.
- The autofill function requires the correct combination of email address and postal code, which limits the possibility of arbitrary access.
- Technical limitations are implemented to complicate automated calls and enumeration attempts.
- All transmission of personal data takes place over encrypted connections (TLS).

The combined technical measures aim to ensure the confidentiality, integrity and availability of personal data.

As part of the continuous security work, the company has decided to introduce additional safeguards in the checkout flow. These measures are intended to be launched urgently and include the following:

- The number of permitted attempts to enter postal codes per e-mail address is limited to a low number.
- If this limit is exceeded, the possibility to use the email address in checkout will be blocked for a limited period of time.
- The customer is notified in case of repeated input attempts.

The purpose of the measures is to further reduce the risk of systematic testing and to increase transparency towards the data subject in the event of abnormal behaviour.

The company has also taken the following organizational measures:

- Internal guidelines for the processing of personal data in checkout and customer systems.
- Limited internal access to personal data based on need and role.
- Continuous risk assessments in the event of changes in technical solutions relating to personal data processing.
- Follow-up of security-related incidents and abnormal behaviours.

The processing of personal data in question is characterised by a risk-based and proportionate security work. Although it is theoretically possible to attempt to derive data through active and divergent behaviour, this requires a procedure that is beyond what can be considered reasonable or probable in practice. All in all, the existing safeguards, combined with the accompanying measures to be implemented, are deemed to ensure an appropriate level of security for the personal data of data subjects.

Motivation for the decision

Applicable provisions, etc.

It follows from Article 32(1) of the GDPR that, 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 for the rights and freedoms of natural persons, the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by the processing.

It follows from Article 32(1)(b) of the GDPR that the controller must have the ability to ensure the ongoing confidentiality, integrity, availability and resilience of its processing systems and services.

It follows from Article 32(2) of the GDPR that, when assessing the appropriate level of security, particular account must be taken of the risks posed by the processing of personal data, in particular the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Recital 75 states that risks to the rights and freedoms of natural persons, of varying likelihood and severity, may arise from the processing of personal data which could, inter alia, result in physical, material or non-material damage, in particular where the processing could lead to identity theft, fraud or financial loss.

Assessment

The complainant states that the company’s processing of his personal data in the function of automatic filling of data entailed a risk of unauthorised access by third parties. The scope of this supervisory case has therefore been limited to

investigating whether the company's processing of the complainant's personal data in the function in question complies with the security requirements laid down by the GDPR in relation to the measures implemented at the time of the complaint.

The company has stated that the purpose of the function is to facilitate for existing customers when purchasing. Furthermore, the company has implemented certain measures in order to prevent abuse of the function. The company has, among other things, implemented measures by partially masking the data, restricting access routes in such a way that the function is only available within the checkout flow, limiting the possibilities for arbitrary access by requiring a combination of data, and introducing technical restrictions that make automated calls and enumeration attempts more difficult.

IMY notes that the protection that the company is required to implement must ensure an appropriate level of security in accordance with Article 32 of the GDPR. This includes ensuring that personal data cannot be misused by unauthorised persons or be accessible for unauthorised processing in an unadulterated manner.

When assessing the appropriate level of security, it is the responsibility of the data controller to pay particular attention to possible risks for the data subject. A possible risk is the exposure of personal data if some of the information required to activate the function is publicly known or readily available. The exposure of personal data on the internet is a particular risk in itself as the data is made available to an unlimited number of natural persons.

Personal data shall be processed in a manner that ensures appropriate security based, inter alia, on their sensitivity. Personal data such as name and address are not sensitive data within the meaning of Article 9 of the GDPR. They are also not specifically worthy of protection (such as, for example, personal numbers) or integrity sensitive data. However, personal data must generally be protected against unauthorised or unlawful processing (Article 5(1)(f) of the GDPR).

Based on the documentation in the case IMY notes that the personal data of the complainant in the function in question has been partially masked with asterisks. IMY considers that partially masked data still constitutes personal data within the meaning of the GDPR, since the possibility of identification remains even if the risk is reduced. IMY further notes that the submission of certain data in the described form with only partial masking does not exclude that unauthorised persons may gain access to the data. Unauthorised access to data concerning name and postal address provided by the data subject to the company is subject to specific risks for the data subject.

In light of this, IMY finds that the measures which the company had implemented at the time of the processing of the complainant's personal data are not such as to achieve an appropriate level of security in relation to the risk of exposure of the complainant's personal data via the internet. IMY concludes that the measures have not sufficiently reduced the risk of such exposure and that, as a result, the processing has not met an appropriate level of security in relation to the risk.

In conclusion, IMY considers that the company has processed the personal data of the complainant in breach of Article 32 of the GDPR by failing to implement

sufficient measures to ensure an appropriate level of security of the complainant's personal data when processing in the function of automatic filling of data.

Choice of corrective measure

Pursuant to Article 58(2)(i) and Article 83(2) of the GDPR, 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 injunctions and prohibitions. In the case of a minor infringement, IMY may, as stated in recital 148, instead of imposing a fine, issue a reprimand pursuant to Article 58(2)(b). Aggravating and mitigating circumstances of the case need to be taken into consideration. These could include the nature, gravity and duration of the infringement as well as past infringements of relevance.

When assessing the choice of corrective measure, IMY takes into account the following. IMY has found that the company has failed in its obligations in relation to the processing of the complainant's personal data at the time of the complaint. This means that IMY, in the context of this supervisory case, has only investigated the company's processing of an individual data subject's personal data. In light of this, and particularly in regards to the fact that the company has not previously been found to have infringed the GDPR, IMY considers this to be a minor infringement within the meaning of recital 148. IMY therefore issues the company a reprimand for the infringement.

[redacted]

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

IT and information security specialist [redacted] has also participated in the handling of the case.

Appendix
The complainant's personal data

How to appeal

If you wish to appeal IMY:s decision, please write to IMY. Please indicate in your letter the decision you wish to appeal and the amendment that you are requesting. The appeal must reach IMY no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, IMY will forward it to the Administrative Court in Stockholm for assessment.

You can send the appeal by email to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. IMY:s contact details are set out on the first page of the decision.