Swedish Authority for Privacy Protection

Notice: This document is an unofficial translation of the Swedish Authority for Privacy Protection's (IMY) draft decision, no. DI-2021-4355. Only the Swedish version of the decision is deemed authentic.

Ref no:
DI-2021-4355

Date of decision:
2023-01-19

Date of translation:
2023-01-19

Decision pursuant to Article 60 under the General Data Protection Regulation – If Skadeförsäkring AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection ("IMY") concludes that If Skadeförsäkring AB, as per 6 November 2020, has processed personal data in violation of Article 32(1) of the GDPR[1] by sending sensitive personal data to the complainant in an e-mail without using a sufficiently secure encryption solution. Hence, If Skadeförsäkring AB has not implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing.

IMY gives If Skadeförsäkring a reprimand pursuant to Article 58(2)(b) of the GDPR for the concluded violation.

Presentation on the supervisory case

IMY has initiated supervision regarding If Skadeförsäkring AB ("If" or "the company") due to a complaint.

The complainant has stated that personal data regarding health has been sent via e-mail without encryption all the way from the sender to the receiver, i.e. by the use of so-called end-to-end encryption. Due to the complaint, IMY has initiated an investigation for the purpose of assessing whether If has ensured an appropriate level of security in accordance with Article 32 of the GDPR as regards the relevant processing.

The investigation in this case has been carried out through written correspondence. Since the complaint concerns cross-border processing, IMY has used the mechanisms for cooperation and consistency contained in Chapter VII of the GDPR. The supervisory authorities concerned have been the data protection authorities in Denmark, Finland, Norway and Estonia.

[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).

What If have stated

If has mainly stated the following.

Transfer of sensitive personal data via e-mail as per 6 November 2020
If has stated that the company is the data controller for the processing of personal data to which the complaint relates. Furthermore, If has stated that, in the context of its claims settlement, the company sent an e-mail to the complainant in one of the complainant's reported personal injury. The e-mail was sent on 6 November 2020 to the e-mail address provided by the complainant. It contained If's decision and an attached file containing the medical assessment which the decision was based upon. The medical assessment included information regarding background, course of events, diagnosis, assessment, graduation of possible invalidity and date of birth (not the social security number).

The e-mail was sent encrypted with so-called Enforced Transport Layer Encryption (Enforced TLS-encryption). This implied that the message was encrypted from If's servers to the recipient's e-mail server, which in the present case was hosted by Tele2 (the operator). In the event that a receiving server was unable to receive a TLS encrypted message, the message was not sent. Thus, it was ensured that the message was always encrypted during transmission. The company's guidelines in force at the time stated that when sensitive personal data were sent by e-mail, the e-mail should always be encrypted.

The solution with enforced TLS encryption was implemented following a decision[2] from the Danish data protection authority, Datatilsynet, where If received criticism for using opportunistic TLS encryption for e-mails containing sensitive personal data.

If also refers to a decision[3] of Datatilsynet in which the Danish data protection authority concluded, following an investigation of a law firm, that the use of enforced TLS 1.2 entails an encryption with sufficient security for e-mails containing confidential and sensitive personal information during transmission. If stated that it was this encryption solution that was used when the e-mail containing the medical assessment was sent to the complainant on 6 November 2020.

New solution for managing e-mail messages
If has stated that, during the period following the complaint, the company has increased its security by, among other things, developing and launching a new communication solution for e-mails that are sent to the company's customers. Within the framework of this solution, If's customers get access to e-mails via "My Pages" on the company's website. The solution works in such a way that a notification is sent to the customer by e-mail or text message informing the customer that the customer has received a message from If that can be read on "My pages". In order to log in to "My pages", the customer needs to authenticate with the Swedish e-identification "BankID".

[2] See Datatilsynet's (Denmark) decision of 18 June 2020 in case J.nr. 2019-31-2175.
[3] See Datatilsynet's (Denmark) decision of 5 November 2019 in case J.nr. 2019-41-0026.

Justification of the decision

Applicable provisions

Data concerning health constitutes so-called sensitive personal data. It is prohibited to process such special categories of personal data pursuant to Article 9(1) of the GDPR, unless any of the exceptions set out under Article 9(2) is applicable to the processing. These data are considered to be worthy of extra protection as the processing of such data may pose significant risks to the fundamental rights and freedom of individuals.

Furthermore, pursuant to Article 32(1) of the GDPR, the controller shall take appropriate technical and organisational measures to ensure an appropriate level of security for the protection of the data being processed. When assessing the appropriate technical and organisational measures, the controller shall take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing and the risks to the rights and freedoms of natural persons.

According to Article 32(1), appropriate safeguards include, among other things:

- The pseudonymisation and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Pursuant to Article 32(2) of the GDPR, when assessing the appropriate level of security, account shall be taken in particular of the risks that are presented 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.

IMY's assessment

E-mail sent to the complainant on 6 November 2020
Since the controller is responsible for the security of the processing pursuant to Article 32 of the GDPR, the controller needs to assess the risks associated with the processing of personal data and take appropriate technical and organisational measures to address the identified risks. What constitute appropriate measures should not be understood as an arbitrary estimation, but an adequate assessment, based on the nature, scope, context and purpose of the processing and the risks to the individual's rights and freedoms. In this case, the issue is the transfer of sensitive personal data over an open network (internet). The processing of sensitive personal data entails that the technical and organisational measures to be taken by the controller are subject to enhanced requirements.

When an e-mail is sent over an open network, the sender or recipient generally has no control over which computers (e.g. servers) the specific e-mail passes along the way. A consequence of this is that anyone who possesses equipment that unprotected e-mails pass through, can access, disseminate or distort them.

By taking appropriate technical and organisational measures, it should not be possible for unauthorised persons to read personal data transmitted over an open network. This can be achieved by encrypting the e-mail containing personal data and/or by protecting the transmission of the e-mail through encryption. Enforced TLS is an example of an encryption solution that can be used to protect an e-mail. In the present case, enforced TLS was used when the relevant e-mail was sent.

IMY notes that the solution used by If to send the e-mail to the complainant only encrypted the e-mail during the transport from If's e-mail server to the e-mail server provided by the complainant's operator. This implied that the encryption ended before the message had reached the final recipient and, thus, did not constitute an end-to-end encryption. Consequently, there was a risk that unauthorised persons could access the e-mail in plain text after the encrypted transmission had ended.

In light of the above, it cannot be deemed that If had protected the data in such a manner that only the intended recipient could access it after the e-mail had been delivered to the operator's e-mail server. At that moment, the encryption ceased and therefore the data lacked sufficient protection against unauthorised disclosure of, or unauthorised access to, the personal data. Since the e-mail contained sensitive personal data, there was a significant risk of breach of the complainant's privacy.

If refers to a decision issued by the Danish data protection authority, Datatilsynet, which concerns a law firm, to demonstrate that Datatilsynet has deemed enforced TLS to be a sufficiently secure solution for transfer of sensitive personal data. IMY notes that the relevant decision does not concern a specific processing, but rather a planned investigation of the security of the processing of personal data, in particular when using encrypted e-mails. The law firm has specified various methods that it uses to ensure secure communication. The method to be applied is assessed in each individual case and one of the methods is to encrypt the transmission of e-mails using enforced TLS. Datatilsynet has assessed that the law firm's action was in accordance with the GDPR. IMY's investigation in this particular case differs from the Danish decision since this investigation concerns the question whether a specific consignment has been adequately protected all the way from the sender to the receiver.

In conclusion, IMY considers that, during the specific occasion, If had not taken appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by the processing, since If had sent the e-mail containing sensitive personal data without ensuring that the deployed encryption solution protected the message all the way to the recipient. Consequently, If processed personal data in breach of Article 32(1) of the GDPR.

If's new solution for managing e-mails

If has stated that, during the period following the complaint, the company has, among other things, developed and launched a new communication solution for e-mails to its customers. It is noted that the personal data processing carried out within the scope of this new solution is not subject of the complaint and is therefore not part of IMY's investigation.

Choice of intervention

Article 58(2) and Article 83(2) of the GDPR give IMY the authority to impose an administrative fine. Depending on the circumstances of the case, an administrative fine shall be imposed in addition to or in place of the other measures referred to under Article 58(2), such as injunctions and prohibitions. Furthermore, Article 83(2) determines the factors to be taken into account when deciding on an administrative fine and 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 under Article 58(2)(b). The aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous infringements of relevance, shall be considered.

IMY has found that If has processed personal data in breach of Article 32(1) of the GDPR. An infringement of that provision may give rise to a fine. If's infringement was committed when the company sent an e-mail containing sensitive personal data to the complainant on 6 November 2020 without using a sufficiently secure encryption solution that protected the message all the way from the sender to the intended recipient (so-called end-to-end encryption).

IMY's investigation concerns an e-mail sent by If without the use of adequate security measures — the one to which the complaint relates. If has worked to improve the security by, following Datatilsynet's decision against If, changing from opportunistic to enforced TLS and also, following the complainant's allegations of security flaws, taking security measures by, among other things, developing and launching a new communication solution for e-mails to the company's customers. Overall, IMY therefore considers the infringement to be minor why, on the basis of 58(2)(b) of the GDPR, If is given a reprimand.

This decision has been approved by unit manager [redacted], following a presentation by It and information security specialist [redacted].

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection. Please indicate in your letter the decision you want to appeal and the amendment that you are requesting. The appeal must reach the Swedish Authority for Privacy Protection no later than three weeks from the date on which you received the decision. If the appeal has been received in due time, the Swedish Authority for Privacy Protection will forward it to the Administrative Court in Stockholm for review. You can send the appeal by e-mail to IMY if the appeal does not contain any sensitive personal data or information that may be subject to confidentiality. The Swedish Authority for Privacy Protection’s contact details are set out in the first page of the decision.