If Skadeförsäkring AB

Diary number:

DI-2021-4355

Date:

2023-01-19

Decision after supervision according to

data protection regulation – If

Damage insurance

The Privacy Protection Authority's decision

The Swedish Data Protection Authority states that If Skadeförsäkring AB, on 6 November

2020, has processed personal data in violation of Article 32.1 of the Data Protection Regulation1.

This has happened because If Skadeförsäkring AB has sent sensitive information to the complainant

personal data about him in an e-mail message without using a sufficiently secure one

encryption solution. If Skadeförsäkring AB has therefore not taken appropriate technical measures

and organizational measures to ensure a level of security that is appropriate in

relation to the risk of the treatment.

The Swedish Privacy Protection Authority gives If Skadeförsäkring AB a reprimand according to article

58.2 b of the data protection regulation for the established violation.

Account of the supervisory matter

The Swedish Privacy Protection Authority (IMY) has started supervision of If Skadeförsäkring AB

(If or the company) due to a complaint.

The complainant has stated that personal data relating to health has been transmitted via e-mail

without having been protected by encryption all the way from the sender to the recipient, i.e.

through a so-called end-to-end encryption. As a result of the complaint, IMY has initiated

supervision in order to investigate whether If has ensured an appropriate level of security in accordance with

Article 32 of the Data Protection Regulation for the current processing.

The proceedings have taken place through an exchange of letters. Against the background that it applies cross-border treatment, IMY has used the mechanisms for cooperation and uniformity found in Chapter VII of the Data Protection Regulation. Concerned regulatory authorities 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 regarding the processing of personal data and on the free flow of such data and on the cancellation of directive 95/46/EC (General Data Protection Regulation).

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

Data from If

If has essentially stated the following.

Transfer of sensitive personal data via e-mail on November 6, 2020

If has stated that the company is the personal data controller for the personal data processing to which the complaint relates. Furthermore, If has stated that within the framework of its claims regulation in one of the complainant's reported personal injury sent an email to it complaining. The email was sent on November 6, 2020 to that email address as stated by the complainant. It contained If's decision as well as an attached file containing it medical assessment that was the basis for the decision. The medical assessment covered background, sequence of events, diagnosis, assessment, grading of any disability and date of birth (not social security number).

The e-mail was sent encrypted with so-called mandatory Transport Layer Security-encryption (Enforced TLS encryption). That meant the message was transmitted encrypted from If's servers to the recipient's e-mail server, which in the current case existed with Tele2 (the operator). In case the receiving server could not receive one TLS encrypted message, it was not sent. In this way it was ensured that the message was always transmitted encrypted. The guidelines that applied at the time in question the time stipulated that when sensitive personal data was sent via e-mail, the e-the mail message is always encrypted.

The solution with mandatory TLS encryption was implemented due to a decision2 from the Danish Data Protection Authority where If received criticism for using so-called opportunistic TLS when encrypting emails that contained sensitive personal data.

If has also referred to a ruling3 from the Danish Data Protection Authority there the data protection authority found, after an examination by a law firm, that the use of mandatory TLS 1.2 means an encryption with sufficient security for e-mail containing confidential and sensitive personal information in transit. If has stated that it was this encryption solution that was also used when e-the medical assessment mail was sent to the complainant on

November 6, 2020.

New solution for managing e-mails

If has stated that, in the time since the complaint, the company has increased security, among other things by the fact that the company has developed and launched a new communication solution for e-postal messages to the company's customers. Within the framework of this solution, If's customers get access to e-mail messages via "My pages" on the company's website. Solution works in such a way that a notification is sent to the customer by e-mail or SMS with information that the customer has received a message from If that can be read on "My pages". To log in to "My Pages", the customer needs to authenticate with BankID.

2 See Datatilsynet's (Denmark) decision of 18 June 2020 in case J. no. 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 regulations

Information about health constitutes so-called sensitive personal data. It is forbidden to treat such special categories of personal data according to Article 9.1 i data protection regulation, unless the processing is covered by one of the exceptions in article 9.2. These data are considered extra protective because the processing of them information may entail significant risks for the fundamental rights of individuals and freedoms.

The personal data controller must further, according to Article 32.1 of the data protection regulation, take appropriate technical and organizational measures to ensure a suitable security level to protect the data being processed. In assessing which

technical and organizational measures that are appropriate it shall

data controllers take into account the latest developments, implementation costs

and the nature, scope, context and purpose of the treatment as well as the risks for

rights and freedoms of natural persons.

According to Article 32.1, appropriate protective measures include, among other things:

• Pseudonymization and encryption of personal data.

• The ability to continuously ensure confidentiality, integrity, availability

and resilience of treatment systems and services.

• The ability to restore the availability and access to personal data i

reasonable time in the event of a physical or technical incident.

• A procedure for regularly testing, investigating and evaluating effectiveness

in the technical and organizational measures that must ensure

the safety of the treatment.

According to article 32.2 of the data protection regulation, when assessing the appropriate

security level special consideration is given to the risks that the treatment entails, in particular

for accidental or unlawful destruction, loss or alteration or for unauthorized disclosure of

or unauthorized access to the personal data transmitted, stored or otherwise

treated.

IMY's assessment

Email sent to the complainant on November 6, 2020

Because the person responsible for personal data according to Article 32 of the Data Protection Regulation

is responsible for the security of the processing, the personal data controller needs

assess the risks associated with the processing of personal data that

must take place and take appropriate technical and organizational measures to manage them

risks that are identified. What are appropriate measures should not be taken as such

the question of an arbitrary assessment without an assessment that is adequate from the outside

the nature, scope, context and purpose of the processing and the risks associated with it

individual freedoms and rights. In this case, it is the issue of the transfer of sensitive

personal data over an open network (internet). That it concerns the treatment of sensitive

personal data means that higher demands are placed on the technical and organizational aspects

measures that the personal data controller must take.

When an e-mail message is sent over an open network, the sender or recipient has i

generally no control over which computers (e.g. servers) the specific e-

the mail passes along the road. A consequence of this is that everyone who

has equipment through which unprotected e-mails pass, can access,

spread or deface them.

By taking appropriate technical and organizational measures, personal data shall

transmitted over an open network cannot be read by unauthorized persons. It can be achieved through

that the e-mail containing personal data is encrypted and/or that

the transmission of the e-mail message is protected by encryption. Forcing TLS is one

example of an encryption solution that can be used to protect an e-

mail message. In the current case, the transmission of the e-mail took place with

forcing TLS.

IMY notes that the solution used by If to transmit the email

to the complainant only the e-mail encrypted in transit from If's e-

mail server to the mail server provided by the complainant's carrier. The

meant that the encryption ended before the message had reached the final

the recipient and thus did not constitute a so-called end-to-end encryption. In that way

there was a risk that unauthorized persons could read the e-mail in plain text after that
the encrypted transmission had ended.

Due to the above, If cannot be considered to have protected the data in such a way
way that only the intended recipient could take part in them after e-
the mail had been delivered to the operator's mail server. At this time
the encryption ended and thus the data lacked sufficient protection against
unauthorized disclosure of or unauthorized access to the personal data. Because it touched
concerned with sensitive personal data, it posed a considerable risk of breach of privacy
against the complainant.

If has referred to a ruling from the Danish Data Protection Authority, which concerns a law firm,
to show that the Norwegian Data Protection Authority has assessed mandatory TLS as a sufficiently secure solution
to transfer sensitive personal data. IMY can state that the decision does not concern one
specific treatment without there being a question of a planned safety inspection
when processing personal data, especially when using encrypted e-
postal messages. The law firm has specified different methods that they use to
ensure secure communication. Which method is used is assessed on a case-by-case basis
the case and one of the methods is to encrypt the transmission of email message through
to use force TLS. The Norwegian Data Protection Authority has assessed that the law firm's actions were in
in accordance with the data protection regulation. The IMY's review in this case differs from that
invoked the ruling as this review concerns whether a specific consignment has
covered by adequate protection all the way from the sender to the recipient.

In summary, IMY finds that If, on the occasion in question, had not taken
appropriate technical and organizational measures to ensure a level of security
which was appropriate in relation to the risk of the treatment, because If sent e-
the postal message containing sensitive personal data without ensuring that it
encryption solution chosen protected the message all the way to the recipient. If

thereby processed personal data in violation of Article 32.1 of the Data Protection Regulation.

If's new solution for managing e-mail messages

If has stated that, in the time since the complaint, among other things, it has developed and

launched a new communication solution for email messages to the company's customers. The

it is noted that the personal data processing that takes place within the framework of this solution does not

is the subject of the complaint and is therefore not part of IMY's review.

Choice of intervention

From article 58.2 i and article 83.2 of the data protection regulation it appears that IMY has

authority to impose an administrative penalty fee. Depending on the circumstances

in the individual case, an administrative penalty fee shall be imposed in addition to or instead of

the other measures referred to in Article 58.2, such as e.g. injunctions and prohibitions. Further

it is clear from article 83.2 which factors must be taken into account when deciding on an administrative

penalty fee shall be imposed and when determining the size of the fee. If it is

in the case of a minor violation, the IMY receives as stated in recital 148 instead of

impose a penalty charge issue a reprimand according to Article 58.2 b. Consideration must be given

aggravating and mitigating circumstances in the case, such as the nature of the offence,

severity and duration and previous violations of relevance.

IMY has established that If has processed personal data in violation of Article 32.1 i

data protection regulation. A violation of that provision may result in a

penalty fee. If's violation has occurred by the company on November 6, 2020

sent an email containing sensitive personal data to the complainant

without using a sufficiently secure encryption solution that protected the entire message

the path from the sender to the intended recipient (so-called end-to-end encryption).

IMY's supervision concerns an e-mail message that If sent without the use of sufficient

security measures – that which the complaint relates to. If has been working on improving

security partly by having changed from the Data Protection Authority's decision against If

opportunistically to forced TLS, partly that after the complainant complained

security flaws have taken security measures by, among other things, having developed and

launched a new communication solution for email messages to the company's customers.

Overall, therefore, IMY considers that it is a matter of a minor violation, why If,

with the support of 58.2 b of the data protection regulation, a reprimand is given.

Miscellaneous

This decision has been made by unit manager Katarina Tullstedt after presentation of IT and

information security specialist Mats Juhlén.

The lawyer Per Nydén also participated in the final handling of the case.

Katarina Tullstedt, 2023-01-19 (This is an electronic signature)

Copy to

DPO@if.se

How to appeal

If you want to appeal the decision, you must write to IMY. State in the letter which decision you made

appeals and the change you request. The appeal must have been received by IMY

no later than three weeks from the day you were informed of the decision. If the appeal has been received

In due course, IMY forwards it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive information

personal data or information that may be subject to confidentiality. The authority's

contact details appear on the first page of the decision.