The Hospital Board in Region Uppsala

751 85 Uppsala

Diary number:

DI-2021-5595

Date:

2022-01-26

Decision after supervision according to

data protection regulation against

The Hospital Board in Region Uppsala

Table of Contents

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

The Privacy Protection Authority's decision

The Swedish Privacy Agency (IMY) states that the Hospital Board in Region Uppsala (hospital board) as personal data controller has, during the period from 25 May 2018 until May 7, 2019, processed personal data in violation of articles 5.1 f and 32.1 i data protection regulation1 as follows:

□

□

The Norwegian Hospital Authority has sent sensitive personal data that was not encrypted via open network to patients and referrers. The treatment has also taken place in combat

with Region Uppsala's own guidelines. This means that the hospital board does not have
taken appropriate technical and organizational measures to ensure a
safety level that is appropriate in relation to the risk of the treatment.
The Norwegian Hospital Authority has stored sensitive personal data in the e-mail hosting service
Outlook. This means that the hospital board has not taken appropriate technical measures
measures to ensure a level of security appropriate in relation to
the risk of the treatment.
IMY decides with the support of articles 58.2 and 83 of the data protection regulation and ch. 6.
Section 2 of the Data Protection Act2 that the hospital board, for violation of articles 5.1 f and 32.1
in the data protection regulation, must pay an administrative sanction fee of 1,600,000 (en
million six hundred thousand) kroner.
Account of the supervisory matter
The starting point for the supervisory case
IMY decided to start an inspection against Region Uppsala due to the region's
notification on 7 May 2019 about a personal data incident.
IMY's review covers the personal data processing carried out by the hospital board
in connection with the Academic Hospital sending e-mails with patient information to
patients and referrers in third countries. IMY's review also covers the storage of
patient details in the email hosting service Outlook.
Within the framework of this supervision, IMY has reviewed the current one
the processing of personal data meets the security requirements set out in articles 5.1 f
and 32 of the data protection regulation. IMY has not reviewed
the processing of personal data is compatible with the regulation in the data protection regulation i
otherwise, for example the provisions on the transfer of personal data to third countries.
The Data Protection Regulation came into force on 25 May 2018. IMY's supervision includes
therefore the period from 25 May 2018 to 7 May 2019 (when the report was received). IMY has

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).

2 The Act (2018:218) with supplementary provisions to the EU's data protection regulation.

3(11)

not reviewed the measures that the hospital board has stated that it took after the 7

May 2019.

Information from the hospital board

The Regional Board in Region Uppsala has stated that it has the right to represent the region

outwards. The hospital board has stated that it agrees with what the regional board stated.

The Hospital Board, through the regional board, has stated, among other things, the following.

Personal data responsibility

The Swedish Hospital Authority is the personal data controller for the personal data processing which

occurs when e-mail is sent from and to patients or referrers abroad. The treatment

takes place at the administration, the Academic Hospital, which is placed under the committee

hospital board. This assessment is made against the background that the hospital board is one

independent administrative authority that determines purposes and means with

the processing of personal data.

E-mail that is sent unencrypted over an open network to third countries

Processing of personal data in e-mail

The academic hospital sends e-mails to patients and referrers (that is

the home hospital) abroad at the patient's or referrer's initiative. It's up to

the patient or the referrer to choose how the data should be submitted. The dialogue between the patient or the referrer and the University Hospital mainly takes place via E-mail.

A patient from abroad who receives care at the University Hospital is registered in the main journal system Cosmic. Journal documents obtained from the patient about their health condition is scanned into Cosmic. Also the care provided at Akademiska the hospital is documented in Cosmic. When the treatment ends, the doctor in charge writes a compilation of care in a so-called Medical report in Cosmic. Medical report sent to the patient or referrer by post, but if it is urgent it is sent via e-mail.

The purpose of the treatment is to provide highly specialized healthcare at Academic Hospital.

The academic hospital sends an estimated 500–1,000 such e-mails per month. The emails were sent in 2018 to patients alternatively remitters in Lebanon, Morocco, Nepal, Pakistan, Peru, Russia, Saudi Arabia, Switzerland, Thailand, Turkey, USA, Argentina, Australia, India, Iraq, Iran, Israel, Canada, Kenya and China.

The e-mails usually contain journal documents and are forwarded to the person concerned operations manager, specialist and in some cases other staff within Akademiska the hospital. Two people have access to the personal data. It is administrative staff with a healthcare background who have access to the personal data and staff subject to confidentiality.

The personal data that is processed is information about health and information about the patient name, reserve social security number, home address, e-mail address, telephone number, sender,

concerned area of activity and time of booked care. Those registered are employees,

patients and children. As regards employees, information about them only appears in

sending and receiving email addresses.

The processing of personal data concerned approximately 300 registered persons per year counted from 2014 onwards

May 2019. The number applies to both people who came in with requests for care and

those treated at the Academic Hospital.

Personal data processing has been ongoing since 2014 and is still ongoing. The

appears from a letter from the hospital board dated 2 June 2021.

Encryption

Personal data is sent unencrypted over an open network. This means that the transfer of

the e-mail and the information in the e-mail messages are not protected by encryption.

Since the introduction of Outlook, the Hospital Board has used Microsoft's

default settings, which means that the transmission of the email takes place with it

the opportunistic cryptographic communication protocol, OTLS3. The Hospital Board

uses version 1.2 of the cryptographic communication protocol (TLS 1.2).

This means that if the recipient's email provider does not have this version of TLS, is selected

a previous version of TLS.

If TLS is not supported by the recipient's e-mail provider, e-mails are sent

the mail messages unencrypted during transmission. According to the hospital board, it concerns approx

1 in 9,000 emails. However, the Swedish Hospital Board has not verified exactly how

many of these emails per day sent unencrypted in this

personal data processing.

The Swedish Hospital Board has not met the requirements for the transfer of personal data in the open

networks must be made in such a way that unauthorized persons cannot access them. This then

the transfer was made unencrypted via Outlook.

Governing document

According to Region Uppsala's policy document on the handling of sensitive e-mails

personal data is not communicated via e-mail.

Actions taken after the incident

The Swedish Hospital Board introduced an encryption solution for files in September 2019, which

enabled a secure transmission via e-mail.

Systematic improvement work is underway and the hospital board has worked with one

risk analysis and a consequence assessment.

Storage in the email hosting service Outlook

In Outlook, the e-mail messages between the patient or sender and Akademiska are stored

the hospital. The journal documents are also stored in Outlook.

3 Opportunistic Transport Layer Security.

Justification of the decision

Applicable rules

The responsibility of the person in charge of personal data

The person who, alone or together with others, determines the ends and the means for

the processing of personal data is the personal data controller. This is apparent from Article 4.7

in the data protection regulation.

The personal data controller is responsible for and must be able to demonstrate that the basic

the principles in Article 5 of the Data Protection Regulation are followed (Article 5.2).

The personal data controller is responsible for implementing appropriate technical and

organizational measures to ensure and be able to demonstrate that the processing is carried out in

in accordance with the data protection regulation. The measures must be implemented taking into account

the nature, scope, context and purpose of the processing and the risks, of

varying degrees of probability and seriousness, for the freedoms and rights of natural persons.

The measures must be reviewed and updated if necessary. It appears from Article 24.1 i

data protection regulation.

The requirement for security when processing personal data, etc.

A fundamental principle for the processing of personal data is the requirement for security

according to article 5.1 f of the data protection regulation, where it is stated that the personal data must

processed in a way that ensures appropriate security for the personal data,

including protection against unauthorized or unauthorized processing and against loss, destruction or

damage by accident, using appropriate technical or

organizational measures.

Information about health constitutes so-called sensitive personal data. It is forbidden to

process such personal data in accordance with Article 9.1 of the Data Protection Regulation, unless

the processing is not covered by any of the exceptions in Article 9.2 of the regulation.

It follows from Article 32.1 of the data protection regulation that the personal data controller and

the personal data assistant must take appropriate technical and organizational measures to

ensure a level of safety that is appropriate in relation to the risk of the treatment.

It must take into account the latest developments, implementation costs

and the nature, scope, context and purpose of the processing as well as the risks, of

varying degree of probability and seriousness, for the rights and freedoms of natural persons.

When assessing the appropriate security level, special consideration must be given to the risks that

the processing entails, in particular from accidental or illegal destruction, loss or

change or to unauthorized disclosure of or unauthorized access to the personal data that

transferred, stored or otherwise processed. It appears from Article 32.2 i

data protection regulation.

Recital 75 of the data protection regulation states the factors that must be taken into account the assessment of the risk to the rights and freedoms of natural persons who may arise when processing personal data. Among other things must be taken into account the processing concerns personal data about health or about vulnerable natural persons, especially children, or if the processing involves a large number of personal data and applies to a large number of registered users.

Recitals 39 and 83 also provide guidance on the more detailed meaning of the data protection regulation's requirements for security when processing personal data.

IMY's assessment

Personal data responsibility

The Swedish Hospital Board has stated that it is responsible for personal data for it personal data processing that takes place when e-mail is sent from the University Hospital to patients and referrers abroad. This is supported by the other investigation in the case.

IMY therefore assesses that the hospital board is responsible for personal data for the e-postal transfers at issue in the case. Furthermore, IMY assesses that The hospital board is also the personal data controller for the personal data processing which occurs when stored in the email hosting service Outlook because the email transmissions takes place from there.

Sensitive personal data has been sent unencrypted via an open network

As the person in charge of personal data, the hospital board must take appropriate technical and organizational measures to ensure a level of security that is appropriate i

relation to the risks (Article 32 of the Data Protection Regulation). The personal data that
processed must, for example, be protected against unauthorized disclosure or unauthorized access.
What is the appropriate security level varies in relation to, among other things, the risks involved
the rights of natural persons that the processing entails and the nature of the processing,
scope, context and purpose. In the assessment, it must, for example,
taken into account what type of personal data is processed, for example information about
health.4
The Norwegian Hospital Authority has sent a large amount of personal data via e-mail to patients and
remitters abroad. It concerns an estimated 500–1,000 e-mails sent
mail messages per month. The emails in question contained
personal health data that is sensitive personal data. Treatment of sensitive
personal data can involve significant risks to personal integrity and
therefore, strong protection is required when processing such data. This means that if
such personal data is sent by e-mail it must be protected in such a way that
unauthorized persons cannot take part in them. The personal data can, for example, be protected by
encryption.
From the hospital board's information, it appears that the hospital board used a technique, so
called OTLS, which means that the transmission of the email is encrypted just in case
receiving mail server supports TLS. If receiving mail server does not support
TLS, the transmission of the email will be unencrypted. This means that the hospital board
uses a technology that is dependent on the recipient's technical settings, which means
that the hospital board cannot ensure that the transmission of the e-mail is encrypted. E-
the post has been sent externally (ie outside the Uppsala Region), which has resulted in
that it was not possible to ensure that the e-mail sent from the Academic Hospital
is received with an encryption that is suitable in relation to the risk of the processing.
The Swedish Hospital Board has itself stated that it has not verified how many of the e-

the mail messages sent unencrypted over the open network per day.

In the current case, the information in the e-mails is sent without encryption, that is

say the information has been able to be read in clear text via an open network (internet). This means that

4 See recitals 75 and 76 of the data protection regulation.

unauthorized persons have been able to access the personal data in the e-mails and that

other than intended recipients have been able to access the data both under

the transfer, in cases where the recipient's email server did not support TLS, and after

the transmission of the email. According to IMY, there is a risk that the data will be leaked

wrong hands after the transfer, because the person sending the data would

able to write an incorrect recipient address [1].

IMY finds that the information in the e-mails should have been protected against unauthorized access

revealing or unauthorized access, and this absolutely regardless of the transmission of the e-mail

been encrypted or not. The Hospital Board should have taken technical measures, to

example in the form of encryption, to protect the personal data and thereby

ensure an appropriate level of protection for the data.

That a large number of sensitive personal data over a long period of time has been exposed to

internet without protection against unauthorized disclosure or unauthorized access, means according to IMY

that the lack of security was of such a serious nature that it also entails a

violation of article 5.1 f of the data protection regulation.

According to the hospital board, Region Uppsala's governing document on the handling of mail is stated

and e-mail that sensitive personal data may not be communicated via e-mail.

The Swedish Hospital Board has thus identified the risks associated with the treatment of sensitive patients

personal data in e-mail entails but has not taken sufficient measures to comply

the guidelines. IMY therefore finds that the hospital board has not taken the appropriate measures

organizational measures required to ensure the security of the processing.

Overall, IMY finds that the hospital board, by not having taken appropriate measures

technical and organizational measures to ensure a level of security that is

suitable in relation to the risk of the processing, has processed personal data in violation

with articles 5.1 f and 32.1 of the data protection regulation.

Sensitive personal data has been stored in Outlook

The Swedish Hospital Board has stated that the medical records are also stored in Outlook in addition

the storage in the main journal system Cosmic.

The journal documents contain sensitive personal health data

personal data. Processing sensitive personal data can mean significant

risks to personal integrity and therefore strong protection is required during treatment

of such data. This means, among other things, that these personal data must

are protected in such a way that unauthorized persons cannot take part in them.

The purpose of an email system (in this case Outlook) is to disseminate and communicate

information. An e-mail system is exposed to the internet, which means that the data in

the system risks becoming accessible to unauthorized persons. Outlook is therefore generally a

inappropriate storage location for sensitive personal data.

By storing journal documents in Outlook, the current data has been exposed to a

high risk that they will be removed or that unauthorized persons will gain access to them. This means that

the hospital board has not taken the technical measures required according to article 32 i

the data protection regulation to ensure appropriate protection for the data.

That a large number of sensitive personal data over a long period of time has been exposed to

internet without protection against unauthorized disclosure or unauthorized access, means according to IMY

[1] See the Swedish Data Protection Authority's report Reported personal data incidents 2019 (report 2020:2).

that the lack of security was of such a serious nature that it also entails a

violation of article 5.1 f of the data protection regulation.

In summary, IMY believes that the hospital board has not taken appropriate technical measures

measures to prevent unauthorized disclosure of or unauthorized access to

the personal data stored in Outlook. The Hospital Board has thereby not

ensured a level of safety that is appropriate in relation to the risk of the treatment.

The Swedish Hospital Board has thus processed the personal data in violation of articles 5.1 f

and 32.1 of the data protection regulation.

Choice of intervention

Legal regulation

In the event of violations of the data protection regulation, IMY has a number of corrective measures

powers to be available according to Article 58.2 a–j of the data protection regulation, among other things

reprimand, injunction and penalty fees.

IMY shall impose penalty fees in addition to or in lieu of other corrective measures

as referred to in Article 58(2), depending on the circumstances of each individual case.

Member States may lay down rules for whether and to what extent administrative

penalty fees may be imposed on public authorities. It appears from Article 83.7 i

the regulation. In accordance with this, Sweden has decided that the supervisory authority shall receive

collect penalty fees from authorities. For violations of, among other things, Article 32 shall

the fee amounts to a maximum of SEK 5,000,000. For violations of, among other things, Article 5 i

regulation, the fee must amount to a maximum of SEK 10,000,000. It appears from ch. 6. 2

§ the Data Protection Act and Article 83.4 and 83.5 of the Data Protection Ordinance.

If a personal data controller or a personal data assistant, with respect to a

and the same or connected data processing, intentionally or by

negligence violates several of the provisions of this regulation, it may

the total amount of the administrative penalty fee does not exceed the amount determined

for the most serious violation. It appears from Article 83.3 i

data protection regulation.

Each supervisory authority must ensure that the imposition of administrative

penalty charges in each individual case are effective, proportionate and dissuasive. The

stated in Article 83.1 of the Data Protection Regulation.

In article 83.2 of the data protection regulation, the factors that must be considered in order to

decide whether an administrative penalty fee should be imposed, but also at

the determination of the amount of the penalty fee. If it is a question of a smaller one

breach will receive the IMY as set out in recital 148 instead of imposing a

penalty fee issue a reprimand according to article 58.2 b of the regulation. Consideration shall

taken into account aggravating and mitigating circumstances in the case, such as that of the violation

nature, severity and duration as well as previous violations of relevance.

Imposition of penalty fee

IMY has assessed above that the hospital board has violated articles 5.1 f and 32.1 i

data protection regulation. Violations of these provisions may, as shown

above, incur penalty charges.

The violations have occurred because the hospital board has sent a large amount

patient details through unencrypted e-mail via open network to patients and referrers i

third countries and by the patient data being stored in Outlook. The personal data
that was processed was sensitive personal data, which means a high risk for them
registered rights and freedoms. The treatments described in the case have taken place
systematically and over a longer period of time. The treatments via e-mail have also taken place in conflict
with Region Uppsala's own guidelines. Taken together, these factors mean that a
penalty charge should be imposed.

IMY considers that the processing via e-mail and the storage refer to two connected ones
data processing according to article 83.3 of the data protection regulation. This because
the treatments relate to the handling of the same personal data in Outlook and refer to
violation of the same provisions.

When determining the size of the penalty fee, IMY must take into account both aggravating factors and
mitigating circumstances and that the administrative sanction fee shall be
effective, proportionate and dissuasive.

It is aggravating that the processing of personal data has been going on for a long time, that is
say during the audited period from 25 May 2018 to 7 May 2019, and that
The hospital board did not promptly take measures to protect the personal data despite
that the hospital board was aware of the shortcomings in security. It is also aggravating
that the treatments included a large amount of health data that was sent unencrypted
via open network and stored in Outlook. It has been estimated between
500 and 1,000 emails per month accessed by unauthorized persons
to via the internet and covered around 300 registered per year. Through the information that
processed, the registered can be identified directly by name, contact details and
information about health. IMY therefore considers that the nature, scope and the
registered person's dependent status gives the hospital board a special responsibility to ensure
an appropriate protection for the personal data, which did not happen.

It is further aggravating that the treatments have taken place systematically and that they took place in

conflict with Region Uppsala's own guidelines that sensitive personal data should not

sent via e-mail.

As a mitigating circumstance, it is taken into account that the hospital board introduced in September 2019

technical measures in the form of an encryption solution for files.

IMY decides on the basis of a collective assessment that the hospital board should impose a

administrative sanction fee of 1,600,000 (one million six hundred thousand) kroner.

This decision has been taken by the general manager Lena Lindgren Schelin after a presentation

by the lawyer Linda Hamidi. In the final proceedings, the Chief Justice David also has

Törngren, unit manager Malin Blixt and IT security specialist Ulrika Sundling

participated.

Lena Lindgren Schelin, 2022-01-26 (This is an electronic signature)

Appendix

Information on payment of penalty fee.

Copy to

The data protection officer.

How to appeal

If you want to appeal the decision, you must write to the Swedish Privacy Protection Authority. Enter in

the letter which decision you are appealing and the change you are requesting. The appeal shall

have been received by the Privacy Protection Authority no later than three weeks from the date of the decision was announced. If the appeal has been received in time, send

The Privacy Protection Authority forwards it to the Administrative Court in Stockholm examination.

You can e-mail the appeal to the Privacy Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.