The Regional Board in Region Uppsala

751 85 Uppsala

Diary number:

DI-2019-9457

Date:

2022-01-26

Decision after supervision according to

data protection regulation against

The Regional 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 Data Protection Authority (IMY) notes that the Regional Board of Governors in Region Uppsala (the regional board) as personal data controller has, during the period from 25 May 2018 until May 7, 2019, processed personal data in violation of Article 32.1 i data protection regulation1. This has happened through the regional board within the region sent sensitive personal data and social security number via e-mail. The transfer of e- the record was encrypted but not the information in the emails. The treatment has also occurred in violation of Region Uppsala's own guidelines. This means that the regional board

has not taken appropriate technical and organizational measures to ensure a

safety level that is 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.

§ 2 data protection law2 that the regional board, for violation of article 32.1 i

data protection regulation, must pay an administrative penalty fee of 300,000

(three hundred thousand) kroner.

Account of the supervisory matter

The starting point for supervision

IMY decided to initiate an inspection against the regional board after a notification about

personal data incident from the regional board on 7 May 2019.

IMY's review covers two categories of personal data processing.

The first category refers to e-mails with patient details that were sent

automated to relevant care administrations within Region Uppsala for, among other things

administration and quality assurance.

The second category refers to e-mails with patient details that were sent

manually to researchers and doctors within Region Uppsala for, among other things, research and

quality follow-up.

IMY has reviewed whether the processing of personal data in the e-mail meets the requirements

security set out in Article 32 of the Data Protection Regulation.

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

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

May 2019.

Information from the regional board

The Regional Board has stated, among other things, the following.

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.



The first category of personal data processing – email that was sent

automated

The statistics database Cosmic Intelligence retrieved personal data from

the main journal system Cosmic. The personal data was then retrieved by Business

Objects that put the information in an excel file. The transfers happened automatically each

month. Business Objects then sent the Excel files to the relevant care administrations

within Region Uppsala, such as the Academic Hospital and the Hospital in Enköping. E-

the postal messages were sent automatically every month to Region Uppsala's e-

postal domains. The e-mails were sent only to authorized persons within it

administration that was affected within Region Uppsala.

The relevant excel files could contain all data from the patient record,

except for the running text from the patient record's free text field. Depending on the type of

report could also include other information, such as waiting times and patient category.

The Excel files also contained information about social security number, name, care unit and

contact date.

About 25 emails were sent each month to about a hundred recipients within

The academic hospital's area of operation. Hundreds of transmitters and receivers within

Region Uppsala had access to the personal data.

The overall purpose of personal data processing has been administration,
for example to correct errors in the operations and to remedy them. In addition, have
the aim has been to develop and secure the quality of the business.
The processing of personal data has been ongoing since 2015 and until the regional board's
notification of the incident to IMY on May 7, 2019. The treatment was stopped completely i
in connection with the discovery of the incident.
The second category of personal data processing – email that was sent
manually
The statistics database Cosmic Intelligence retrieved personal data from
the main journal system Cosmic. The Diver output system then retrieved personal data
from Cosmic Intelligence and the patient administrative systems IMX and PAS. Socket
of personal data was then done manually from Diver to excel files. The manual ones
the withdrawals were made by, among other things, system developers and the administrator at
regional office. These excel files were then sent to doctors when requested
data for quality follow-up purposes and to researchers when they have requested it
research basis. The emails were only sent to recipients who were
employees within Region Uppsala, i.e. only to Region Uppsala's e-
postal domains. This means that the emails were not sent to email addresses
linked to Uppsala University.
The Excel files could, among other things, contain information about social security numbers, diagnosis codes,
contact date, area of activity, age, county, action code and department. The Excel files
did not contain information about names. The Excel files concerned only patients who were treated
at the Academic Hospital.
About 200−250 e-mails were sent per year. Hundreds of transmitters and
recipients within Region Uppsala had access to the personal data.
The personal data was processed for administrative purposes and to develop and secure

the quality of the business and for research purposes.



4(10)

Personal data processing took place from September 2014 until the regional board's notification about the incident to IMY on May 7, 2019. Treatment was completely stopped in connection with that the incident was discovered and work started to develop a solution for encryption of e-mail.

Information relating to both personal data processing

Personal data responsibility

The Regional Board is the personal data controller for the personal data processing concerned compilation of data in Business Objects and for the processing that takes place at automatic transfer via e-mail. The processing takes place at the administration regional office, which is placed under the board of the regional board. This assessment is made against background of the fact that the regional board is an independent administrative authority which determines the purposes and means of personal data processing.

The Regional Board is also responsible for personal data for the processing that takes place in Diver and for the processing that takes place via the manual transmission via e-mail.

The Regional Board has attached the documents Regulations for boards and committees i Region Uppsala and the Regional Board's delegation order.

Governing document

According to Region Uppsala's governing document on the handling of mail and e-mail, sensitive items are received personal data is not communicated via e-mail.

Categories of registrants

Categories of registered are employees, patients, children and persons with protected

identity. As far as employees are concerned, information about them only appears in broadcasting and recipient email addresses.

The personal data processing affects a total of between 100,000 and 500,000 individuals for the period 2015−2019.

Categories of users

The categories of users who have access to the personal data are administrative personnel with access to source systems and storage areas.

Encryption

The transport (transmission) of the e-mail within the region was encrypted but the information in the excel files was not protected by encryption.

The transport of the email was sent encrypted with the cryptographic the TLS1.2 communication protocol to recipients within Region Uppsala.

In the first personal data processing, the Regional Board used a local e-mail server when transporting the e-mail between Business Objects and recipients within the region. In the second reading, the regional board used Microsoft's Outlook for e-the mail.



There were no technical safeguards to prevent reading and modification of the information in the excel files. There was also a lack of safeguards to prevent that unauthorized access to the information.

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 of Article 5 of the Data Protection Regulation are followed (Article 5.2 of the Regulation).
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.
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 of the Data Protection Regulation that the person in charge of personal data 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 factors that must be taken into account in the assessment of the risk to the rights and freedoms of natural persons. Loss of, among other things, is mentioned confidentiality with regard to personal data subject to confidentiality and whether the processing concerns information about health or sexual life. Further must be taken into account the processing concerns personal data about vulnerable natural persons, especially children, or if the processing involves a large number of personal data and applies to a large number of registrants.

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.



6(10)

IMY's assessment

Personal data responsibility

The Regional Board has stated that it is responsible for personal data for the e-postal transfers described in the case, which is supported by the investigation in the case. IMY therefore assesses that the regional board is responsible for the personal data of those in question the treatments.

Sensitive personal data has been sent unencrypted within the region

The Regional Board has sent excel files with patient data within the region via e-mail. Regarding the first category of personal data processing, approximately 25 e-mails automatically every month and in the case of the second category about 200-250 emails were sent manually per year. The transfer of e-the record within the region was encrypted but not the information in the excel files.

The Regional Board has stated that sensitive personal data may not be communicated via e-mail according to Region Uppsala's steering document on the handling of mail and e-mail.

As the personal data controller, the regional 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 and freedoms of natural persons that the processing entails as well as the nature, scope, context and purpose of the treatment. In the assessment must for example, it is taken into account what type of personal data is processed, to for example if it concerns information about health.3

The Excel files in question contained sensitive personal health data personal data. Processing sensitive personal data can mean significant risks to personal integrity. In addition, the excel files contained social security numbers which are considered to be particularly protective personal data4. The data in e-the mails were therefore of such a nature as to require strong protection.

The transmission of the e-mail from the regional board was encrypted, but not the information in it the emails. This meant that the information in the excel files could not be intercepted (read) during the actual transfer. However, the information could be read in plain text by both authorized and unauthorized recipients after the transfer. At an automated transfer, there is a certain risk of data falling into the wrong hands if the system would update incorrectly. In the case of a manual transfer of personal data, there is still one higher risk of the data falling into the wrong hands compared to an automated one transfer. This is because the person sending the data could write one incorrect recipient address5. According to IMY's assessment, the regional board should have taken action technical measures, for example in the form of encryption, to protect the information in them

automated and the manual emails against unauthorized disclosure or

unauthorized access and thereby ensure an appropriate level of protection.

According to the regional 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.

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

4 See article 87 of the data protection regulation and ch. 3 Section 10 of the Data Protection Act.

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



The Regional Board has thus identified the risks that the treatment of sensitive

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

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

organizational measures required to ensure the security of the treatment.

Overall, IMY finds that the regional board has not taken appropriate technical and

organizational measures to ensure a level of security that is appropriate i

relation to the risk of the treatment. The Regional Board has therefore processed

personal data in violation of article 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) of the Data Protection Regulation, depending on the circumstances i

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. It appears from ch. 6. Section 2 of the Data Protection Act

and Article 83.4 of the Data Protection Regulation.

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 regional board has violated Article 32.1 i

data protection regulation. Violations of that provision may, as stated above,

incur penalty charges.



8(10)

The violations have occurred because the regional board has sent a large amount
unencrypted patient data within the region through encrypted email.
The personal data in the e-mail included sensitive personal data and
social security number, which meant a high risk for the freedoms and rights of the registered.
The treatments have taken place systematically and over a longer period of time. The treatments have
also occurred in violation of Region Uppsala's own guidelines. These factors mean
overall, that a penalty fee should be imposed.
IMY states that the manual and the automatic transmission of e-mail
constitutes connected data processing according to Article 83.3 i
data protection regulation. This is because the treatments concern patient information such as
was taken from the main journal system Cosmic for similar purposes such as
administration and quality assurance. In addition, there is the issue of violation of
the same provision, i.e. Article 32.1 of the regulation.
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, during the audited period from 25 May 2018 to 7 May 2019,
and that they have taken place systematically. It is also aggravating that the treatments included
a large amount of health data that unauthorized persons were able to access after the transfer.
As for the first category of personal data processing, it has been about

about 25 e-mails per month that unauthorized people have been able to access and as far as the second category is concerned, it has been around 200−250 e-mail messages per year. The Regional Board estimates that the personal data processing in total has touched between 100,000 and 500,000 individuals for the period 2015−2019. It is thus a question of a large number of registered users during a year. Through the data processed, the registered can be identified directly through, for example, name, social security number and health information. IMY therefore considers that the nature, scope and dependent status of the data subjects provide the regional board a special responsibility to ensure appropriate protection for the personal data, which did not happen.

It is further aggravating that the treatments took place in conflict with Region Uppsala's own guidelines that sensitive personal data should not be sent via e-mail.

As mitigating circumstances, IMY considers that the transmission of the e-mail was encrypted and that the email was sent internally within the region. This means that the regional board has taken certain measures with the aim of complying with the requirements and reducing the risks of the treatments. IMY also considers that the regional board stopped the treatments in connection with the notification of a personal data incident to IMY on 7 May 2019.

IMY decides based on an overall assessment that the regional board must pay a administrative sanction fee of 300,000 (three 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.