The Regional Board of Region Skåne

291 89 Kristianstad

Diary number:

IMY-2022-1290

Your diary number:

2022-JUR000018

Date:

2023-04-26

Decision after supervision according to

data protection regulation –

The Regional Board of Region Skåne

The Privacy Protection Authority's decision

The Swedish Data Protection Authority (IMY) notes that the Regional Board of Governors in Region Skåne (the region) in its capacity as data controller has processed personal data in violation with Article 32.1 of the Data Protection Regulation1 in that the region has stored unencrypted personal data about patients on a USB stick and on November 1, 2020 lost control over the USB stick. The region has thereby treated sensitive personal data without having ensured an appropriate level of security in relation to the risk for loss, unauthorized disclosure of or unauthorized access to the personal data.

IMY decides with the support of articles 58.2 and 83 of the data protection regulation and ch. 6. 2 § data protection act2 that the region must pay an administrative sanction fee for violation of Article 32.1 of the Data Protection Ordinance of 200,000 (two hundred thousand) crowns.

Account of the supervisory matter

Starting point for supervision

IMY received from the region on 18 November 2020 a notification of a

personal data incident that took place on November 1, 2020. The report shows that a

usb stick containing social security number and sensitive personal data of 1,934

recorded was forgotten by a staff member in the pocket of clinical clothing placed in a

laundry bag for transport to regional laundry.

IMY has subsequently received two complaints regarding the personal data incident.

Against this background, IMY decided to initiate supervision.

IMY has reviewed the processing of personal data on the USB stick in question

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

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 Act (2018:218) with supplementary provisions to the EU 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 the region

The region has submitted two statements together with the following documents.

•

Instruction for Region Skåne's processing of personal data, version 2.0,

drawn up on 20 June 2018 and revised on 11 December 2020.

• Information Security Guidelines, dated December 7, 2017.

•

Instruction for the application of guidelines for information security, dated 22

May 2020.

• Create and store DIGITAL AND ANALOG INFORMATION, version 2.2,

dated April 22, 2016.

• Requirements for system support for handling and storage of digital documents, version

1.0, dated December 18, 2020.

• Delegation order for the regional board, dated 9 February 2023.

• Delegation decision regarding Region Skåne's opinion

The Data Protection Authority's supervision according to the data protection regulation IMY-

2022-1290, dated 21 February 2023.

• Application for register data, from quality registers, for research purposes,

signed on May 26, 2020.

• Decision on extradition, signed on 24 June 2020.

• Instruction Annual Wheel for Region Skåne's information security coordinator,

listed as Exhibit 3 and undated.

• Processing of personal data for research, version 1.1, dated 20 May

2018.

The following is essentially what emerges from the first opinion from the region.

The personal data controller is the legal entity Region Skåne and the regional board
is ultimately responsible for the organization Region Skåne's processing of personal data.
There are two types of personal data on the missing USB stick; social security number and
special categories of personal data attributable to Article 9.1 i
the data protection regulation in the form of information on health concerning 1,934 registrants.
Regarding the special categories of personal data listed in Article 9.1 i
data protection regulation contains information about health. The health information is attributable to a
procedure-related quality register, SCAAR, regarding coronary artery disease. The data
is information about health of the "biodata" type. The data is unencrypted, but the majority of
the values are written as ones and zeros representing "yes" or "no" and stand
thus not in plain text. Employees in the region are allowed to use removable media in form
of usb for processing personal data on decided organizational and technical
protective measures are taken. The region's governing document prescribed as technical protection
measures when storing and transporting storage media that the protection must correspond to it
protection value that the information has based on the information classification that
carried out and that storage media containing information worthy of protection must
protected against unauthorized access, misuse or tampering during transport. At
mandatory training of the employees informs the region that usb should be avoided but
that employees when using usb for storing sensitive or valuable information must
use encrypted usb. These can be ordered internally. The missing USB stick has
not recovered despite extensive work to recover it. The search of
the usb stick has happened over a longer period of time (November 2020 – March 2021). The investigation in
the case does not indicate that the information has been disseminated or that unauthorized persons have received it
the information because the USB stick was present within the organization, but then it was not
found, it is reasonably safe to assume that an accessibility violation has taken place.
The Swedish Privacy Protection Authority

The following is essentially what emerges from the second opinion from the region.

The personal data on the missing USB stick came from a national quality register, SCAAR. Requests for removal from the quality register are handled by Uppsala clinical research center, UCR. The researcher employed by Region Skåne had applied for a withdrawal and received a decision on the release of register data from quality register SCAAR for research purposes. UCR describes in the application that Submitted material must be stored in a secure manner, in encrypted form so that unauthorized persons cannot access it. Responsible researcher, employed by the research leader Region Skåne has accepted and committed to them security measures that the central personal data controller has set up for the disclosure of the relevant personal data.

Region Skåne's use of storage media is followed up annually in accordance with instructions Annual wheel for Region Skåne's information security coordinator. A technical one security measure deployed in 2021 since the current event is 7-zip. 7-zip is a compression program that can also be used to encrypt files. One additional technical security measure taken is the development of a storage area, Secure external storage, for handling sensitive personal data, confidential data or other information deemed privacy-sensitive and worthy of protection and which is intended to be shared with parties outside Region Skåne. Organizational security measures have also been taken due to the personal data incident.

Region Skåne is carrying out an ongoing review of the instruction Processing of personal data for research and intends, among other things, to update the instruction with clarifying references to decided existing technical security measures.

The Regional Service administration has also introduced stricter procedures for the units Laundry and textile and Customer Center regarding the handling of found objects at the laundry. In order to further strengthen the compliance of the decided technical and organizational the security measures, in addition to the activities described above and in earlier opinion, the Skåne University Hospital administration has intensified it data protection legal support to the research organization.

Region Skåne certainly admits that the personal data incident involved a breach of the data protection regulation and has therefore decided on compensation for those affected data subjects who requested it, in accordance with the obligation in Article 82.1 i data protection regulation. The violation of the data protection regulation in this regard does not mean, however, that Region Skåne has either breached its responsibility as personal data controller or in the security measures taken, without the breach is solely due to the negligence of an individual employee.

Justification of the decision

Applicable rules, etc.

Personal data and the responsibility of the data controller

Article 4.1 of the data protection regulation defines the concept of personal data as any information relating to an identified or identifiable natural person.

Information about health is defined in Article 4.15 of the Data Protection Regulation as personal data relating to a natural person's physical or mental health, including provision of healthcare services, which provide information about his health status.

Information about health constitutes so-called sensitive personal data.3 Also information such as indirectly may reveal sensitive personal data constitutes a processing of sensitive personal data according to article 9.1 of the data protection regulation.4 European The Swedish Data Protection Board (EDPB) has stated that the concept of information about health according to the data protection regulation must be interpreted broadly against the background of, among other things, the EU the court's judgment in the Lindqvist case and as it appears from reason 53 to data protection regulation that information about health deserves comprehensive protection.5

According to Article 4.7 of the Data Protection Regulation, the person in charge of personal data is a physical or legal person, public authority, institution or other body which alone or together with others determines the purposes and means of the processing of personal data. If the purposes and means of the processing are determined by Union law or the national law of the Member States can the personal data controller or the special criteria for how he is to be appointed are prescribed in Union law or in national law of the Member States. The personal data controller is responsible for and must be able to demonstrate that the basic principles in Article 5 of the Data Protection Regulation are followed, it appears from article 5.2 of the data protection regulation.

According to Article 5.1 f of the data protection regulation, the personal data must be processed in one ways that ensure 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.

Furthermore, it appears from article 24.1 that the person in charge of personal data is responsible for implement appropriate technical and organizational measures to ensure and be able to show that the processing is carried out in accordance with the data protection regulation. The measures must be carried out taking into account the nature, scope, context and purpose and the risks, of varying degree of probability and seriousness, for physical people's freedoms and rights. The measures must be reviewed and updated if necessary.

Reason 74 of the data protection regulation states that personal data controllers should
are held responsible for all processing of personal data that they carry out or that is carried out on
on their behalf. Personal data controllers should in particular be required to take appropriate and
effective measures and be able to demonstrate that the treatment is compatible with
the data protection regulation, also in terms of the effectiveness of the measures. The
personal data controllers should take into account the nature of the processing within these measures,
scope, context and purpose as well as the risk to the rights of natural persons
and freedoms.

The EDPB has stated that in principle all processing of personal data by employees that takes place
within the framework of an organization's activities can be considered as taking place under
that organization's control. Employees who, for example, have access to personal data
within an organization are generally not considered "data controllers" or
"personal data assistants", but rather as "persons acting under it".
the authority of the personal data controller or personal data assistant" in the sense that
referred to in Article 29 of the Data Protection Regulation. In exceptional cases, however, it may happen that a
employee decides to use personal data for his own purposes and thereby

3 CJEU case C-101/01, Lindqvist, EU:C:2003:596, paragraph 51.

4 CJEU case C-184/20, Vyriausioji tarnybinės etikos komisija, EU:C:2022:601, paragraph 128.

5 EDPB guidelines 03/2020 on the processing of data on health for scientific research purposes in connection with
the covid-19 outbreak, p. 5.

illegally exceeds the powers he or she was given (for example to start
his own company or similar).6

The requirement for security when processing personal data, etc.

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.

Appropriate security measures may include, among other things, pseudonymization and encryption of personal data.

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 39 of the data protection regulation states, among other things, that personal data should processed in a manner that ensures appropriate security and confidentiality for the personal data and prevents unauthorized access to and unauthorized use of personal data and the equipment used for processing.

Recital 75 of the data protection regulation states factors that should 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.

Recital 83 of the data protection regulation provides further guidance on it in more detail the meaning of the data protection regulation's requirements for security when processing personal data, including that personal data controllers should evaluate the risks with the processing and take measures, such as encryption, to reduce them. At

the assessment of the data security risk should also take into account the risks that

personal data processing entails, such as destruction, loss or changes through

accident or unauthorized acts or unauthorized disclosure of or unauthorized

access to the personal data that has been transferred, stored or otherwise processed,

above all when this can cause physical, material or immaterial damage.

IMY's assessment

The investigation into the case shows that the region has lost a USB stick. USB stick

stores unencrypted personal data about health and social security numbers about 1,934

registered. The USB stick has not been found.

Personal data responsibility

The region has indicated that they are responsible for personal data for the current processing

but at the same time believe that they have not breached their responsibility as the violation is due

on an employee's negligence.

6 See the European Data Protection Board's (EDPB) guideline 07/2020 regarding the concepts of personal data controller and

personal data controller in the GDPR, version 2.0, adopted on July 7, 2021, point 19 and article 24.1 of

data protection regulation.

IMY notes the following. Article 4.7 of the data protection regulation states, among other things

that a personal data controller is a natural or legal person, public authority,

institution or other body that alone or together with others decides

the purposes and means for the processing of personal data. Personal data controller

must, according to Article 5.2 of the data protection regulation, be responsible for and be able to demonstrate that

the principles of Article 5.1 are complied with (principle of responsibility). Furthermore, it appears

of Article 24.1 that it is the person in charge of personal data who must carry out the appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with the data protection regulation.

IMY notes that the region determined the purpose and means of the treatment of the personal data in the present case, that is, how and why the personal data should treated. It is thus the region that is responsible for personal data processing of personal data.7 The fact that the region is responsible for personal data means that they are responsible for to comply with the data protection regulation when processing personal data. That responsibility also includes the requirements for the security of the data. The treatment that takes place within the activity is the responsibility of the person in charge of personal data even if it is the question of mistake or misjudgment made by, for example, an employee. It is first about it employees act for other purposes that are not covered by the employer's purposes such as it may be the case that the employee or someone else is responsible for personal data for the treatment. In this case, both have the storage of sensitive personal data on one unencrypted usb and the loss of the usb stick occurred within the scope of the employee's service. The region is thus responsible for the processing of the personal data taking place in in accordance with the data protection regulation's requirements for security.

The treatment involved a high risk

As a personal data controller, the region must take appropriate technical and organizational measures measures to ensure a level of security that is appropriate in relation to the risks with the processing, see Article 32 of the Data Protection Regulation. The personal data that processed must, for example, be protected against loss, unauthorized disclosure or unauthorized access. What is the appropriate level of security varies in relation to, among other things, the risks to 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 is a question of information about health.8

Patients may be considered to have a high expectation that unauthorized persons should not be able to access them information that appears in contact with care. That because patients have the right to a confidential contact with healthcare.9 Processing of personal data within health and healthcare generally entails a high risk for the freedoms and rights of the registered.

On the USB stick in question, the region stores information about health that is sensitive personal data. Processing sensitive personal data can mean significant risks to personal integrity. In addition, the USB stick contains social security numbers which are considered to be particularly protective personal data. 10 The processing of the data on the USB stick is therefore of such a nature that the data requires strong protection.

7 Cf. EDPB's guideline 07/2020 regarding the concepts of personal data controller and personal data processor in the GDPR, version 2.0, adopted on 7 July 2021, paragraphs 19 and 27.

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

9 Within both individual and general healthcare activities, information about an individual's state of health or other personal conditions of confidentiality, see ch. 6. Section 12 of the Patient Safety Act (2010:659) and ch. 25 § 1 the Publicity and Confidentiality Act (2009:400).

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

The region has not taken sufficient security measures

IMY states that the current processing means that storage has taken place personal data on a USB stick without these being protected by suitable security measures such as encryption. Encryption means that the protectable the information is converted from a readable to an encoded format using a

encryption key. The information then becomes unreadable to anyone who does not have access the encryption key. This means that the information worth protecting cannot be read out directly where this is stored without an encryption key.

The investigation shows that directly and solely from the data on the lost USB the memory can be deduced to relate to information about health linked to patients' social security number, i.e. it is possible to identify that the registered persons have been subject to care and treatment. IMY further notes that although some of the values are inscribed like ones and zeros to represent yes or no, that doesn't take away from it moving on information about health and which can be linked to an identifiable person.

When personal data is processed on removable storage media, such as USB, there is significant risks of personal data being spread unintentionally. The security measures to be taken based on assessment according to Article 32 i the data protection regulation means that the processing of privacy-sensitive personal data must not be lost, disclosed without authorization or disseminated in an unintended manner. The region is responsible as the personal data controller for these personal data processed in a way that ensures appropriate security, which includes protection against unauthorized or unauthorized processing and against loss, destruction or damage by accident. That the region stored health data on an unencrypted USB stick like those also lost means that there is a significant risk that someone who does not have the right to take part of them may gain access to the data. This in turn means that it also there is a risk that the information may be spread further. The region thus does not have ensured an appropriate level of security in relation to the risk of loss, unauthorized disclosure of or unauthorized access to the personal data.

Overall, IMY finds that the region 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 by the region having used a removable

medium for storing sensitive personal data without ensuring that unauthorized persons do not can take part in them and then lose control over the USB stick. The region therefore has processed personal data in violation of article 32.1 of the data protection regulation.

Choice of intervention

Applicable regulations

From article 58.2 and article 83.2 of the data protection regulation it appears that IMY has power to impose administrative penalty charges in accordance with Article 83.

Depending on the circumstances of the individual case, administrative penalty fees are imposed in addition to or instead of the other measures referred to in article 58.2, such as injunctions and prohibitions. Furthermore, it is clear from article 83.2 which factors to be taken into account when deciding whether administrative penalty charges are to be imposed and when determining the size of the fee. If it is a minor violation in accordance with what is stated in recital 148, instead of imposing a penalty fee, the IMY may issue a reprimand according to article 58.2 b. Consideration must be given to aggravating and mitigating circumstances circumstances of the case, such as the nature, severity and duration of the infringement as well as previous violations of relevance.

The 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 data protection regulation. Sweden has accordingly decided to the supervisory authority shall be allowed to collect sanction fees from authorities. For violations of among other things, article 32, the fee must amount to a maximum of SEK 5,000,000. It is clear from 6 Cape. Section 2 of the Data Protection Act and Article 83.4 of the Data Protection Ordinance.

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.

A penalty fee must be imposed

IMY has assessed above that the region has violated Article 32.1 of the data protection regulation.

Violations of that provision can, as stated above, lead to sanctions

fees. IMY finds in an overall assessment of the circumstances described

under the heading Amount of the penalty fee that there is reason to impose on the board a

penalty fee and that it is therefore not a question of such a minor violation that

there is reason to issue a reprimand instead.

The size of the penalty fee

For violations of, among other things, Article 32 of the Data Protection Ordinance may

the sanction fee for public authorities amounts to a maximum of SEK 5,000,000. The

appears from ch. 6. Section 2 of the Data Protection Act and Article 83.4 of the Data Protection Ordinance. IN

the assessment of the seriousness of the violation is taken into account by IMY in accordance with Article 83.2 g i

data protection regulation that the processing has included sensitive personal data about

health.

Furthermore, IMY takes into account what has emerged about the nature of the violation, degree of severity

and duration based on what is stated in article 83.2 a of the data protection regulation.

The violation has occurred because the region has stored unencrypted personal data about

patients on a USB stick and lost control of the USB stick. It has meant that

the region has not ensured an appropriate level of security in relation to the risk of loss,

unauthorized disclosure of or unauthorized access to the personal data. The treatment has

meant that a larger number of patients can be identified directly by social security number

together with information about health, which means a high risk for the data subjects' freedom

and rights. That the region has not met the safety requirements is serious because it

is the issue of personal data of such a type that the data requires strong protection

based on the nature of the treatment.

It also refers to personal data that is protected by confidentiality. In light of that

the region stated that there are 1,934 registered, it can also be stated that

the breach affects a large number of registered users.

IMY considers it an aggravating circumstance that the USB stick was not found and

it is unclear how the personal data has been disseminated.

IMY decides based on an overall assessment that the region must pay an administrative fee

sanction fee of 200,000 (two hundred thousand) kroner.

The Swedish Privacy Protection Authority

Diary number: IMY-2022-1290

Date: 2023-04-26

This decision has been made by the acting head of unit Linn Sandmark after

presentation by the lawyer Anna Hellgren Westerlund. At the final processing

of the case, unit manager Katarina Tullstedt participated. In the processing of

IT and information security specialist Joyce Wong participated in the case.

Linn Sandmark, 2023-04-26 (This is an electronic signature)

Appendix

Information on payment of penalty fee

Copy to

The data protection officer

The appellant

How to appeal

If you want to appeal the decision, you must write to the Swedish Privacy Agency. 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.