The Health and Medical Services Board in Region Dalarna

Diary number:

IMY-2022-695

Your diary number:

HSN 2022/1069

Date:

2023-01-17

Decision after supervision according to

data protection regulation – Health and

the health care board in Region Dalarna

The Privacy Protection Authority's decision

The Swedish Privacy Agency (IMY) notes that the Health and Medical Board i

Region Dalarna (the board) from 6 May 2021 to and including 6 July 2022 has

processed personal data in violation of article 32.1 of the data protection regulation1, by

not to take appropriate technical and organizational measures to ensure a

appropriate level of protection in connection with the sending of physical invitations to certain healthcare visits

within Region Dalarna.

IMY decides with the support of ch. 6. Section 2 of the Data Protection Act2 and Articles 58.2 and 83 i

the data protection regulation that the board must pay an administrative sanction fee of

200,000 (two hundred thousand) kroner.

Account of the supervisory matter

IMY has initiated supervision of the board due to information that emerged in one

complaint from a person who, on 6 May 2021, received an invitation via letter to a healthcare visit

within Region Dalarna. The complaint states that the summons was in a window envelope and that

information that it was a summons, the complainant's name and address and the care facility

ning the summons was fully visible in the window of the envelope. The purpose of IMY's supervision is to investigate the board's processing of personal data in connection with the use of the current type of window envelope for invitations to healthcare visits meets the requirements for security in connection with the processing according to article 32 of the data protection regulation.

Within the framework of the supervisory matter, IMY has only reviewed the committee's mailing of summonses regarding the Child and Adolescent Medical Clinic Mora, Call Center children and young people Falun and the Sleep Laboratory in Avesta.

The board has essentially stated the following. The board is a healthcare provider and personal responsible for the personal data processing that the supervision refers to. Summons from Region Dalarna is sent using Postnord Strålfors AB's (Strålfors) function e letter. The notices are sent securely in digital format from Region Dalarna's journal system to Strålfors, which mechanically prints, envelopes and sends the invitation to the addressee.

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.

Mailing address:
Box 8114
104 20 Stockholm
Website:
www.imy.se
E-mail:
imy@imy.se
Phone:
08-657 61 00

The board identified the risk of using double windows when the service
was procured and therefore bought an additional service which means that envelopes which only
contains a window with the recipient's address to be used. On these envelopes is written
Region Dalarna's postal address printed where the sender's address is usually placed and
the name of the clinic/department that sent the summons is therefore not shown. The board's
opinion is that the sending clinic should not appear on the envelope.

In a statement to IMY dated 28 April 2022, the committee stated that it had started a
investigation together with Strålfors. In an opinion dated 16 June 2022, the board stated i
mainly the following. It is unclear when the committee started sending summons where the patient's
name and the care facility to which the summons refers appear on the window of the envelope.
The investigation shows that the additional service where the sender is hidden only applies to sending
of a maximum of five A4 sheets. If the mailing contains more A4 sheets, a larger envelope is required
be used and then there are no customer-unique envelopes in the assignment that has been signed
eBREV, standard envelopes with two windows are used instead. In the same opinion stated
the committee that the investigative work to review the flow regarding the sending of summonses via
eBREV and risks linked to these that could generate a personal data
incident in progress. In parallel with this, a discussion is being held with Strålfors about the need to
renegotiate the customer assignment to ensure that the correct type of envelope, with hidden
sender, used for all mailings.

In an opinion dated June 16, 2022, the board stated that the treatment that is
subject to supervision had not ceased. In a supplement that the board submitted to IMY
on July 6, 2022, it was stated that the board, until an agreement is reached

with Strålfors, will change the template for invitations to visit the three units
(Children's and youth medicine clinic Mora, Children's consultation clinic and
young Falun and the Sleep Laboratory in Avesta) that have been identified send invitations with
attachments exceeding five A4 sheets. The board has attached a picture that shows that
the invitations will be sent in an envelope with two windows, where Region Dalarnas
postal address appears in one window and information that it is a visit
via video link and the patient's name and address in the second.

In an opinion dated August 9, 2022, the board stated that previous answers have been deleted
from invitations sent through the Take Care IT system. It is about 2,500
summons per year, which corresponds to 0.5 percent of the total number of summons sent
through the current system.

Justification of the decision

Applicable regulations

Scope of the Data Protection Regulation

Article 2.1 of the data protection regulation states that the regulation must be applied to
such processing of personal data that is wholly or partially carried out automatically
as well as on other than automatic processing of personal data that is part of or will be
to be included in a register.

In doctrine, it is stated that since the data protection regulation includes partially automated
processing of personal data, the regulation is applicable in the case of disclosure on paper of
personal data that is in data format.3 Furthermore, the Chancellor of Justice has assessed that

3 See Öhman, Data Protection Regulation (GDPR) etc. (October 13, 2022, Version 2A, JUNO), Comment to article
2.1 subsection Automated processing.

the expression "fully or partially automated processing of personal data" in the present

the repealed Personal Data Act (1998:204) covered the sending of documents by post

when the underlying processing of the personal data was automated.4

Personal data is defined in Article 4.1 of the Data Protection Regulation as any information

which refers to an identified or identifiable natural person.

Processing is defined in Article 4.2 of the Data Protection Regulation as an action or

combination of measures concerning personal data or sets of

personal data, regardless of whether it is performed automatically or not, such as collection,

registration, organization, structuring, storage, processing or modification,

production, reading, use, disclosure by transmission, dissemination or

otherwise providing, adjusting or combining, limiting, erasing

or destruction.

Personal data responsibility and the principle of accountability

According to Article 4.7 of the data protection regulation, the person in charge of personal data means a

natural or legal person, public authority, institution or other body which

alone or together with others determines the purposes and means of treatment

ling 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.

According to ch. 2 Section 6 of the Patient Data Act (2008:355), PDL, is a care provider personal data-

responsible for the processing of personal data carried out by the care provider. In a region or

a municipality is any authority that provides health care personal data-

responsible for the processing of personal data carried out by the authority.

According to Article 5.2 of the Data Protection Regulation, the person in charge of personal data shall be responsible

for and be able to demonstrate that the principles in Article 5.1 are complied with (the principle of liability).

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 degree 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.

Data on health

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. It is prohibited to process such personal data according to Article 9.1 of the Data Protection Ordinance ning, unless the processing is covered by one of the exceptions in Article 9.2 i the regulation.

4 See JK decision 2020-05-18, dnr 3850-19-4.3.2.

Recital 35 of the data protection regulation states the following. Personal information about health should include all the information relating to a registered person's state of health which provides information about the data subject's past, present or future physical or mental health conditions. This includes information about the natural person who

collected in connection with registration for or provision of health and
healthcare services to the natural person according to the European Parliament and the Council
directive 2011/24/EU, a number, a symbol or a characteristic such as the physical
the person assigned to identify him for health care purposes, data
arising from tests or examination of a body part or body substance,
including genetic information and biological samples, and other information about, for example
disease, disability, risk of disease, medical history, clinical treatment or the
recorded physiological or biomedical conditions, regardless of the source, for example
show from a doctor or other healthcare professional, a hospital, a medical technician
product or an in vitro diagnostic test.

In the Lindqvist case (C-101/01, EU:C:2003:596, point 51), the European Court of Justice has determined that
information that a person has injured their foot and is on part-time sick leave constitutes a person-
data relating to health according to the data protection directive5 (the directive was repealed by
data protection regulation). The European Court of Justice stated in the case that with regard to the purpose of
the data protection directive, the expression "data relating to health" should be given a broad interpretation and
considered to include data relating to all aspects of a person's health, both physical and
psychological ones (see point 50). The European Court of Justice has further in a later ruling
Vyriausioji tarnybinės etikos komisiya (C-184/20, EU:C:2022:601) stated that
the concept of sensitive personal data according to article 9.1 of the data protection regulation shall
interpreted broadly and judged that even personal data that indirectly reveals a physical
a person's sexual orientation constitutes sensitive personal data according to the person in question
the provision.

The European Data Protection Board (EDPB) has stated that the concept of health data
according to the data protection regulation must be interpreted broadly against the background of, among other things, EU
the court's judgment in the Lindqvist case and as it appears from reason 53 to the data protection
the regulation that information about health deserves extensive protection6. IMY has in one

legal position deemed that information about guardianship according to the parental code

are information about health (IMYRS 2022:3).

The requirement for security when processing personal data

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

alteration or unauthorized disclosure of or unauthorized access to personal data which

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

data protection regulation.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regarding the processing of personal data and the free flow of such data.

6 See the EDPB's guidelines 03/2020 on the processing of data on health for scientific research purposes in connection

with the covid-19 outbreak, p. 5.

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.

In recital 76 of the data protection regulation, it is stated that how likely and serious the risk is for it data subject's rights and freedoms should be determined based on the nature of the processing, scope, context and purpose. The risk should be evaluated on the basis of a objective assessment, through which it is determined whether the data processing includes a risk or high risk.

If the personal data controller hires a personal data assistant to carry out a processing, the personal data controller shall only employ personal data assistants who provides sufficient guarantees to implement appropriate technical and organizational actions. It must take place in such a way that the processing meets the requirements of data protection regulation and that the data subject's rights are protected. It appears from article 28.1 and recital 81 of the data protection regulation.

The Swedish Privacy Protection Authority's assessment

The investigation into the matter shows that the board during the period from 6 May 2021 to and including on 6 July 2022 has used a service for sending physical letters which meant that some invitations to health care visits have been sent out in window envelopes with information that it is a summons, the patient's name and address and the care facility to which the visit relates were fully visible.

The Data Protection Regulation is applicable

The information in the summons that was visible through the window envelopes refers to identified persons. It is therefore a matter of personal data. The board's processing of the personal data consists of a series of measures where the board's disclosure of personal data by physical mail has been a part. The underlying part of the process, which, among other things, means that invitations are sent in digital format from

Region Dalarna's journal system is automated. IMY therefore assesses that it is a question
about a partially automated processing of personal data covered by
scope of application of the data protection regulation.

Personal data responsibility

The board has stated that it is the healthcare provider responsible for personal data for that treatment
of personal data in the event of invitations to healthcare visits within the Dalarna Region that are subject to
supervision, which is supported by the other investigation in the case. IMY therefore assesses that
the committee is responsible for personal data for the current processing.

The treatment involved a high risk

As a personal data controller, the board must, according to Article 32.1 of the Data Protection Ordinance,
ning, take appropriate technical and organizational measures to ensure a
appropriate level of security in relation to the risks involved in processing personal data. The
also applies when personal data is processed by a personal data processor. IMY does
following assessment of the risks of the current treatment.

According to information from the board, summonses that have shown sender reception have been sent
from the Child and Adolescent Medicine Clinic Mora, Children's Call Center
and young Falun and the Sleep Laboratory in Avesta. The investigation into the matter shows that
the clinics offer care for children and young people aged 0–17 with illnesses and
illness that requires more specialist knowledge and resources than is normally available
care centre, help for children and young people up to 17 years of age with mild to moderate mental illness
respective investigation and treatment of various sleep disorders.

IMY states that the concept of health must be interpreted broadly and assesses that the care which

given at the care facilities in question is so specific that an invitation to visit someone
of these receptions may be considered to provide information about the individual's physical or
mental health conditions.
Against this background, IMY assesses that the information regarding these care facilities,
which were fully visible at the time of dispatch, constitute information about health in the sense referred to in
Article 4.15 of the Data Protection Regulation. The data are therefore so-called sensitive
personal data covered by the protection according to Article 9.1 of the regulation.
The data is also protected within the health and medical care by confidentiality according to
25 ch. Section 1 of the Publicity and Confidentiality Act (2009:400). Because two of the concerned
the care facilities only provide care for people who are 17 years of age or younger
furthermore, it is established that in some cases the information has also referred to children, who are considered special
protected according to the data protection regulation7. It is also a comprehensive one
treatment that includes approximately 2,500 mailings from several different care facilities.
Against this background, IMY assesses that it is a treatment that involved a
high risk and that strong protection was therefore required.
The board has not taken sufficient security measures
IMY states that the mailings with invitations to visits at Children's and Youth Medicine's
should the reception Mora, the Children and Young People's Call Reception Falun and
The sleep laboratory in Avesta took place in such a way that the sensitive personal data
have been fully visible to everyone who came into contact with the letters. The data has been
available to, for example, those who work with handling mail, those who share
household with the recipient and the person who received a letter that was delivered to the wrong address.
In order to achieve an appropriate level of security, the dispatches should, according to IMY's assessment, have
took place in such a way that the sensitive personal data was not visible. The committee
has thus not been able to ensure the security level required according to Article 32.1
in the data protection regulation.

It can be stated that the board's opinion is indeed that it should not be apparent from
the envelope which reception a summons to a care visit refers to and that the board therefore
procured a service for the purpose of concealing sending reception. After IMY started supervision
however, the committee carried out an investigation which showed that the service in question only
included invitations on a maximum of five A4 sheets and that other invitations were sent in envelopes
which showed which clinic the visit was for. IMY states that it has arrived at
the committee as personal data controller to ensure that before the processing in question, it
the current add-on service fulfilled the need to keep the data hidden from others yet
the recipient of the letter.

7 See recital 38 of the data protection regulation.

Against this background, IMY assesses that the committee has not taken sufficient measures
to ensure a level of security appropriate to the risk involved
current treatment. The board has therefore processed personal data in violation of
article 32.1 of the data protection regulation.

Choice of intervention

Applicable regulations

In the event of violations of the data protection regulation, IMY has a number of corrective powers
called to be available according to Article 58.2 a–j of the data protection regulation, including reprimand,
injunction and penalty fees.

Article 83.2 of the data protection regulation states that IMY must impose administrative
penalty fees in addition to or instead of the other measures referred to in Article 58.2
depending on the circumstances of the individual case. Member States may determine

rules for whether and to what extent administrative penalty charges can be imposed

public authorities. This is apparent from article 83.7 of the data protection regulation. According to

6 ch. Section 2 of the Data Protection Act allows IMY to collect penalty fees from authorities at

violations referred to in article 83.4, 83.5 and 83.6 of the data protection regulation and that

Article 83.1, 83.2 and 83.3 of the regulation shall then be applied.

In article 83.2 of the data protection regulation, the factors that must be taken into account when making a decision are stated

if administrative penalty fees are to be imposed and when determining the fee

size. If it is a question of a minor violation, IMY receives according to reason 148 more

data protection regulation to issue a reprimand instead of imposing a penalty fee.

The factors specified in Article 83.2 of the Data Protection Regulation must also be taken into account

the determination of the amount of the penalty fee. Each supervisory authority must ensure

that the imposition of administrative penalty charges is effective in each individual case,

proportionate and dissuasive. This is apparent from Article 83.1 of the Data Protection Ordinance.

A penalty fee must be imposed

IMY has concluded that the committee has processed personal data in violation of Article

32.1 of the data protection regulation. IMY finds in an overall assessment of the

circumstances described under the heading Amount of the penalty fee that there is

reason to impose a penalty fee on the board and that it is therefore not a question of one

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, IMY considers in accordance with Article 83.2 g

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

health and information about children, which are particularly worthy of protection according to data protection

the regulation.

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. Thereby it can be established that the violation has been going on for a longer period of just over a year, from and with May 6, 2021, when the patient who filed the underlying complaint for the supervisory authority received its summons, up to and including 6 July 2022, when the board took

measures to hide the sender's receipt on the envelope when mailing. Against background of the fact that the committee stated that it is about 2,500 summonses per year can also it is established that the violation affects a large number of registered users. Furthermore, it means the fact that the violation has occurred in healthcare - i.e. a business there the registered patient is in a dependent and vulnerable position i relationship with the person in charge of personal data - that there is reason to look more seriously the violation. However, IMY assesses that there are also factors that speak to the contrary direction in the assessment of the seriousness of the infringement. First, it moves if a physical handling and not a digital one which would have involved a risk of greater and faster dissemination of the data. A distribution by regular mail is more limited and controlled than a transfer via the open network. Furthermore, have emerged that the committee identified the risk of exposing those in question the personal data during mailings and therefore took certain measures in order to comply the requirements and reduce the risks of the treatment.

IMY decides based on an overall assessment of the circumstances of the case that The health care board in Region Dalarna must pay an administrative fee

penalty fee of SEK 200,000.

This decision has been taken by the general manager Lena Lindgren Schelin after a presentation by the lawyer Maja Welander. In the final processing of the case has also head of law David Törngren, acting head of unit Linn Sandmark and IT- and information security specialist Magnus Bergström participated.

Lena Lindgren Schelin, 2023-01-17 (This is an electronic signature)

Copy to

The board's 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, Privacy Protection sends the authority forwards it to the Administrative Court in Stockholm for review.

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.