Decision

Diary no

2020-05-11

DI-2020-1539

The Health and Medical Services Board in the Region

Örebro county

The Health Care Board in Region Örebro County –

supervision according to the data protection regulation

The Swedish Data Protection Authority's decision

The Data Inspectorate notes that the Health and Medical Services Board in the Region

Örebro County between September 2019 and January 2020 processed

personal data in violation of Article 5, Article 6 and Article 9 i

data protection regulation. This by having published sensitive

personal data on Region Örebro County's website without it being compatible

with the principles of purpose limitation and task minimization, without

there was a legal basis for it and contrary to the prohibition of processing

sensitive personal data. The Health and Medical Board in Region Örebro County

has also processed personal data in violation of the same publication

article 87 of the data protection regulation and ch. 3 Section 10 of the Act (2018:218) with

supplementary regulations to the EU data protection regulation

(Data Protection Act) by having processed social security numbers without support

for it.

The Data Inspectorate notes that the Health and Medical Services Board in the Region

Örebro County at the review in February 2020 was found to be processing

personal data in violation of Article 32 of the Data Protection Regulation by

not having taken sufficient organizational measures to ensure that

personal data is protected from unauthorized publication on the region's website,

such as establishing written instructions and ensuring that the person who

publish personal data on the website do so in accordance with

the instructions.

Datainspektionen decides with the support of articles 58.2 and 83 i

data protection regulation and ch. 6 Section 2 of the Data Protection Act to Health and

the health board in Region Örebro County for the violations of Article 5,

article 9 and article 32 of the data protection regulation and ch. 3 Section 10

the data protection act must pay an administrative penalty fee of 120,000

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

crowns. Of this amount, SEK 80,000 refer to the violations of articles 5,

6 and 9 and ch. 3 Section 10 of the data protection regulation and SEK 40,000 refers

the violation of Article 32.

Datainspektionen orders with the support of article 58.2 d i

the data protection regulation, the Health and Medical Board in Region Örebro County

to establish written instructions and introduce routines that ensure that

whoever publishes personal data on open websites does so i

in accordance with the instructions.

Account of the supervisory matter

The Data Inspectorate received a complaint against the Health and Medical Board i

Region Örebro county regarding a notification to the JO against forensic psychiatric the clinic in Örebro had been published in its entirety on the region's open website. The publication had taken place before a board meeting on 25 September 2019. The notification contained the identity of the notifier (including social security number), contact details, information that the notifier was admitted to the forensic psychiatric clinic and information that the notifier was subject to urine sampling. Due to this, the Data Inspectorate decided at the end of January 2020 to initiate an inspection against the Health and Medical Care Board i Region Örebro County for the purpose of investigating the committee's handling of personal data in the case of web publications. In connection with the initiation of supervision and the Swedish Data Protection Authority drew the committee's attention to the publication the board removed the publication to which the complaint related.

The health care board in Region Örebro County has essentially stated following.

The published document was immediately removed from the open website. Furthermore, all published invitations and minutes were reviewed in order to check that further disclosure had not taken place. Then one was made personal data incident notification to the Swedish Data Protection Authority, an internal a notification of deviation was drawn up and it was investigated what could be done for that something like this would not happen again.

Region Örebro County normally publishes personal data in summonses and minutes on its website relating to elected politicians or officials in their official/fiduciary duties. When web publishing

Region Örebro län is deemed to be able to invoke public interest in publishing minutes and summonses, including personal data, based on Article 6 i the data protection regulation and ch. 2 Section 2 of the Data Protection Act. Sensitive personal data according to article 9 of the data protection regulation and ch. 3 Section 3 the data protection act must never be published on the region's website. In the present the case should not have been published.

The Health and Medical Services Board lacks written procedures regarding publication of documents and personal data on the website. There are a few people whose task is to publish the health and medical care board's notices and minutes on the website. Procedures for publication are shared orally. In this case, the oral procedures have not been followed and the action was published by mistake.

Region Örebro County has begun work on creating written guidelines and routines for serving notices and minutes to elected officials and for publication on the website.

Other things that emerged in the case

The Swedish Data Protection Authority has reviewed the information provided by the committee about the incident in a personal data notification (dnr PUI-2020-339). The committee states in this document, among other things, that the incident occurred due to "The human factor: error in the individual case" (a suppressed response option), that the act removed from the external web, that removal of the act was accompanied by an immediate review of all published summonses and minutes to ensure that disclosure has not occurred on other way or in other documents, that a date has been set for information and briefing to the staff group concerned regarding rules for publication on the web, and that the data subject has been informed of the incident.

In an appendix to the notification of a personal data incident, the region wrote the following.

"Region Örebro County considers it very important that personal data
is processed correctly and in accordance with the rules applicable at any time.
Therefore, Region Örebro län strives to, in the various steps in the preparation of
cases, pay attention to the existence of personal data in different types of
documents, and that if it is not necessary that they be there, either take
remove them or present them in such a form that they cannot be derived
separate individual. This work takes place systematically and through a number of
preparatory steps./…/In the present case, however, it has been the case that they

the current information as a result of a mistake, which does not normally have
was noticed in the preparation process, has been included in the publication on
the public web."

Justification of decisions

The Swedish Data Protection Authority notes that among the personal data that
was published on Region Örebro County's open website, there was information that
have been sensitive according to Article 9 of the Data Protection Regulation. This applies to
the information that the registered person is admitted to the forensic psychiatric hospital
the clinic and that he is subject to urine sampling. This then the
the former information reveals that the person may suffer from a serious mental illness
disorder and the latter information that the person has or has had one
drug problem. Thus, they constitute information about health. Furthermore, have
social security number covered by the publication.

Legal regulation

Personal data may only be processed if there is a legal basis for it
as stated in Article 6 of the Data Protection Regulation. Such legal support
may for example consist in the fact that the processing is necessary to carry out a
task of public interest, for example giving the public access to it
municipal operations. Processing of sensitive personal data is as
main rule prohibited and such personal data may only be processed
the processing is subject to an exception in Article 9 of the Data Protection Regulation.
Social security numbers may only be processed with the support of ch. 3. Section 10
the data protection law, i.e. if there is (one according to
the provisions of the data protection regulation valid) consent or if
the processing is clearly justified with regard to the purpose of
the treatment, the importance of secure identification or anything else worth considering
reason.
Those who process personal data must also have a legal basis
always comply with the basic principles set out in Article 5 i
data protection regulation. Among other things, personal data may only be used
for specific, explicitly stated and justified purposes (the principle of
purpose limitation) and no more personal data may be processed yet
necessary for the purposes (task minimization principle). Of Article 32

follows that the personal data controller has to take appropriate technical and
organizational measures for personal data to ensure a
security level that is appropriate in relation to the risk to natural persons
rights and freedoms. Furthermore, the personal data controller must, according to

article 32.4, take measures to ensure that every natural person who performs
work under the supervision of the personal data controller, and who may
access to personal data, only processes these on instructions from it
personal data controller.

Datainspektionen's assessment of the publication

The Swedish Data Protection Authority assesses that the publication of a private person's
correspondence to an authority went beyond a conceivable purpose to
publish parts of the current case on the web (giving the public access to
the municipal activities). Thus, there has been nothing special,
explicitly stated and justified purpose of the publication of the relevant ones
the personal data. Furthermore, there has been no legal basis to
publish the personal data and the publication has not been covered by anything
exception to the ban on processing sensitive personal data.

Social security numbers have been published without the conditions stated in ch. 3. Section 10
the data protection act has been fulfilled.

The Health and Medical Services Board has only worked with oral
instructions to the employees responsible for publishing the committee's
documents on the web. The publication should have been preceded by an assessment of
if it was permitted under the data protection regulation. That this has not happened indicates
that the board violated the instructions to those who work under the board
supervisor. This means that the committee has not taken appropriate measures
organizational security measures to protect against unauthorized publication of
personal data on the web.

The Swedish Data Protection Authority has a series of decisions on municipalities' web publications
according to the Personal Data Act1 stated that an appropriate organizational measure for
to protect personal data from improper publication are written procedures for

web publishing. Such routines must be used by the staff and should

determine when personal data may be published, who shall do so

The Personal Data Act (1998:204), PuL, entered into force on 24 October 1998 and ceased to

apply on 24 May 2018. Datainspektionen was the supervisory authority according to PuL until

The Data Protection Regulation came into force on 25 May 2018.

the assessment, how long the data must be kept on the web, work routine for

masking of sensitive or confidential information, handling of linked

document and indication of who is responsible for publication and

possible deletion of data.2 Other appropriate measures may be to see

to ensure that the staff receives sufficient training in the data protection regulation and how

it must work so that personal data is not handled in violation of the regulations.

Such training can ensure that whoever publishes personal data on

the website does this in accordance with the instructions provided by it

personal data controller.

The routines that the health and medical care board had have not been enough to

protect personal data from publication in violation of the data protection regulation.

Adequate measures have not been taken to ensure that those who

publishes personal data under the board's supervision, does so in accordance

with the board's instructions for publication.

The Data Inspectorate therefore states that the Health and Medical Board i

Region Örebro County has violated articles 5, 6, 9 and 32 i

the data protection regulation, and ch. 3 Section 10 of the Data Protection Act.

Choice of intervention

The Swedish Data Protection Authority has found that the committee has published sensitive information personal data and social security number on Region Örebro County's website and that the board lacks written procedures for web publishing. The publication that has taken place has lacked a legitimate purpose and legal basis. The publication has not been covered by any of the exceptions to the prohibition on processing sensitive personal data. This means that the committee has processed personal data contrary to the principles of purpose limitation and data minimization in Article 5 of the Data Protection Regulation, the provision on lawful treatment in Article 6 and the prohibition of treatment of sensitive personal data in Article 9. The publication of social security numbers does not comply the conditions in ch. 3 Section 10 of the Data Protection Act and therefore contravenes it the provision.

Article 58 of the data protection regulation lists all of the Data Protection Authority powers. The Swedish Data Protection Authority has, in the event of violations of

2

See for example DI-1309-2011, DI-1787-2011 and DI-1057-2016.

the data protection regulation a number of corrective powers to be available according to article 58.2 a -j, including reprimand, injunction and penalty fees.

It follows from Article 58.2 of the data protection regulation that the Data Inspectorate i pursuant to Article 83 shall impose penalty charges in addition to or in lieu of other corrective measures referred to in Article 58(2), depending the circumstances of each individual case. If it is a question of a smaller one

violation the supervisory authority, according to reason 148 i

data protection regulation, issue a reprimand instead of imposing one

penalty fee.

A penalty fee must be paid

The Swedish Data Protection Authority has assessed that the board has violated articles 5, 6, 9

and 32 of the data protection regulation and ch. 3 Section 10 of the Data Protection Act, adopted

on the basis of Article 87 of the Data Protection Regulation. These items are covered

of articles 83.4 and 83.5. In the event of a breach of these shall

the regulator consider imposing administrative penalty charges

in addition to, or instead of, other corrective actions.

The Swedish Data Protection Authority assesses that this is not a minor violation.

This in light of the fact that the personal data that was published was sensitive

and touched a patient. Further, the person could not reasonably expect to

his correspondence was made available to a large circle. In addition, was

the personal data published for a long time without it being discovered by

the committee. There is no reason to replace the penalty fee with someone else

Corrective Action. The Health and Medical Services Board must thus be imposed a

administrative penalty fee.

Determining the size of the sanction amount

According to Article 83.1 of the Data Protection Regulation, each supervisory authority must

ensure that the imposition of administrative penalty charges in each individual

case is effective, proportionate and dissuasive.

For authorities, according to ch. 6, § 2 second paragraph of the Data Protection Act that

the penalty fee shall be set at a maximum of SEK 5,000,000 at

violations referred to in article 83.4 of the data protection regulation and at most

SEK 10,000,000 for violations referred to in Article 83.5. Violations of

article 5, 6, 9 and 3 chap. Section 10 of the Data Protection Act (which was adopted on the basis of Article 87) is covered by the higher penalty fees according to Article 83(5) and

violations of Article 32 are covered by the lower maximum amount according to Article 83.4.

In article 83.2 of the data protection regulation, factors to be taken into account are stated determining the size of the penalty fee. These factors include a) the nature, severity and duration of the infringement, b) about the infringement taken place with intent or through negligence, c) the actions that it personal data controller has taken to alleviate the damage that they registered suffered, d) the degree of responsibility of the personal data controller with taking into account the technical measures implemented in accordance with Article 32, g) the categories of personal data covered by the violation, h) it way in which the infringement came to the attention of the supervisory authority, in particular whether and to what extent the personal data controller notified the violation.

In Datainspektionen's assessment of the amount of the penalty fee, take into account taken to the following.

The breach has concerned sensitive personal data concerning a person i dependency for which the publication of the data may have been given serious consequences. Furthermore, the information has been published openly on the region's website for an extended period of time. That there was a lack of appropriate technical and organizational measures to ensure that such personal data does not published poses a risk of similar events occurring again.

The lack of appropriate security measures is reflected in the fact that the board does not discovered the incorrect publication myself. However, the publication has not happened intentionally and there is nothing to indicate that more than one person in the reality would have been affected by erroneous publications of sensitive personal data. The board will add to this as soon as it becomes aware of it if the event acted by removing the published document, inform the data subject and inform the relevant personnel and to work has begun on developing written routines. The Swedish Data Protection Authority also states that the region has filed a personal data incident notification on behalf of the committee to the Data Inspectorate and followed the regulations that exists in that regard.

The publication of personal data on the board's open website refers to a and the same conduct and includes violation of Articles 5, 6 and 9 i the data protection regulation and ch. 3 Section 10 of the Data Protection Act.

The penalty fee for the violation of Article 32 refers to the board's organizational security measures when publishing on open websites and is thus determined separately.

The Data Inspectorate decides based on a collective assessment that Health and The health board in Region Örebro County must pay an administrative fee penalty fee of SEK 120,000 for violations of articles 5, 6, 9 and 32 of the data protection regulation and ch. 3 Section 10 of the Data Protection Act. Of this amount refers to SEK 80,000 for the violations of Articles 5, 6 and 9 of the data protection regulation and ch. 3 Section 10 of the Data Protection Act and 40,000

kronor refers to the violation of Article 32 of the data protection regulation.

Order on further organizational measures

According to Article 58.2 d, the Swedish Data Protection Authority has the authority to submit a personal data controller to ensure that a treatment takes place in accordance with the provisions of the data protection regulation. It appears from article 58.2 that administrative penalty charges can be combined with injunctions.

The Health and Medical Services Board has not taken sufficient organizational measures measures under Article 32 of the Data Protection Regulation to ensure that personal data is protected from unauthorized publication on the region's website, such as establishing written instructions and ensuring that the person who publish personal data on the website do so in accordance with the instructions.

The Health and Medical Board in Region Örebro County shall therefore be ordered to draw up written instructions and introduce routines that ensure that the who publish personal data on open websites do so in accordance with the instructions.

This decision has been made by the director general Lena Lindgren Schelin after presentation by [lawyer] Elin Hallström. At the final processing also has chief legal officer Hans-Olof Lindblom, unit manager Malin Blixt and unit manager Katarina Tullstedt participated. IT security specialist Magnus Bergström has participated in the assessments relating to information security.

Lena Lindgren Schelin, 2020-05-11 (This is an electronic signature)

Appendix

How to pay penalty fee

Copy for the attention of:

The data protection officer

How to appeal

If you want to appeal the decision, you must write to the Swedish Data Protection Authority. Enter in the letter which decision you are appealing and the change you are requesting.

The appeal must have been received by the Swedish Data Protection Authority no later than three weeks from the day the decision was announced. If the appeal has been received in time the Swedish Data Protection Authority forwards it to the Administrative Court in Stockholm for examination.

You can e-mail the appeal to the Swedish Data 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.