Decision

Diarienr

2020-05-11

DI-2020-1539

The Health and Medical Care Board in Region

Örebro County

The Health and Medical Care Board in Örebro County Region -

supervision under the Data Protection Regulation

The Data Inspectorate's decision

The Data Inspectorate states that the Health and Medical Care Board in the Region

Örebro County between September 2019 and January 2020 treated

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

the 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 data minimization, without

there was a legal basis for it and in violation of the ban on treatment

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

has at the same publication also processed personal data in violation of

Article 87 of the Data Protection Regulation and Chapter 3 § 10 law (2018: 218) with

additional provisions to the EU Data Protection Regulation

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

for it.

The Data Inspectorate states that the Health and Medical Care Board in the Region

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

personal data in breach of Article 32 of the Data Protection Regulation by:

have not taken sufficient organizational measures to ensure that

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

such as drawing up written instructions and ensuring that the person

publishes personal information on the website does so in accordance with

the instructions.

The Data Inspectorate decides on the basis of Articles 58 (2) and 83 i

the Data Protection Ordinance and Chapter 6 § 2 of the Data Protection Act that Health and

the Health Care Board in the Örebro County Region for the violations of Article 5,

Article 9 and Article 32 of the Data Protection Ordinance and Chapter 3 § 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

Phone: 08-657 61 00

kronor. Of this amount, SEK 80,000 refers to the violations of Articles 5,

6 and 9 and ch. 3 Section 10 of the Data Protection Ordinance and SEK 40,000 refer to

infringement of Article 32.

The Data Inspectorate submits pursuant to Article 58 (2) (d) i

the Data Protection Ordinance The Health and Medical Care Board in the Örebro County Region

to establish written instructions and establish procedures to ensure that

anyone who publishes personal information on open websites does so in

in accordance with the instructions.

Report on the supervisory matter

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

Region Örebro County regarding a report to the Ombudsman against forensic psychiatry 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 the 25th September 2019. The notification contained the notifier's identity information (including social security number), contact details, information that the notifier was posted on the forensic psychiatric clinic and information that the complainant was the subject of urine sampling. Due to this, the Data Inspectorate decided in the end of January 2020 to initiate a supervision against the Health and Medical Care Board in Örebro County Region in order to investigate the board's handling of personal data for web publications. In connection with the initiation of supervision and the Data Inspectorate alerted the board if the publication took place the board removed the publication to which the complaint concerned.

The Health and Medical Care Board in the Örebro County Region has mainly stated following.

The published document was immediately removed from the open site. Furthermore, all published summonses and minutes were examined in order to check that no further disclosure had taken place. Then one was made personal data incident report to the Swedish Data Inspectorate, an internal The non-conformance report was prepared and it was investigated what could be done for that something similar would not happen again.

The Örebro County Region normally publishes personal data in summonses and minutes on its website relating to elected politicians or employees in their service / trust assignments. For web publishing

The Örebro County Region is considered to be able to invoke a general interest in publishing minutes and summonses, including personal data, based on Article 6 i the Data Protection Ordinance and ch. Section 2 of the Data Protection Act. Sensitive personal data in accordance with Article 9 of the Data Protection Ordinance and Chapter 3. § 3 The Data Protection Act should never be published on the region's website. In the current In this case, publication should not have taken place.

The Health and Medical Care Board lacks written routines 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. Routines for publication are shared orally. In this case, the oral procedures and the document have not been followed was published by mistake.

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

Other information that has emerged in the case

The Data Inspectorate has reviewed the information provided by the board about the incident in a personal data report (dnr PUI-2020-339). The committee states in this document, among other things, that the incident occurred due to "Human factor: error in the individual case" (a pre-printed alternative answer), that the document has been removed from the external web, to be removed by the document was accompanied by an immediate review of all published notices and minutes to ensure that disclosure has not occurred otherwise or in other documents, that a date has been set for information and review to the relevant staff group regarding rules for publication on the web, and that the data subject has been informed of the incident.

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

“Örebro County Region considers it very important that personal data

treated correctly and in accordance with the rules in force at any given time.

Therefore, Region Örebro County 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 way that they can not be traced to

separate individual. This work is done systematically and through a number

preparation 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 have in the usual way

noticed in the preparation process, has followed out in the publication on

the public web. ”

Justification of decision

The Data Inspectorate finds that among the personal data that

was published on Region Örebro County's open website, there was information that

have been sensitive in accordance with Article 9 of the Data Protection Regulation. This is the case for

the information that the data subject is admitted to the forensic psychiatric ward

the clinic and that he is subject to urine sampling. This then it

The former information reveals that the person may be suffering from a serious mental illness

disorder and the latter information that the person has or has had one

drug problems. Thus, they constitute information about health. Further has

social security number covered by the publication.

Legal regulation

Personal data may only be processed if there is a legal basis for it
as set out in Article 6 of the Data Protection Regulation. Such legal support
may, for example, consist in the treatment being necessary to perform one
task of general interest, such as providing the public with transparency
municipal activities. Processing of sensitive personal data is like
as a general rule prohibited and such personal data may only be processed again
processing is covered by an exception in Article 9 of the Data Protection Regulation.
Social security numbers may only be processed with the support of ch. § 10
the Data Protection Act, ie if there is (a according to
the provisions of the Data Protection Regulation are valid) consent or if
the treatment is clearly justified with regard to the purpose of
the treatment, the importance of a secure identification or something else noteworthy
reason.
Those who process personal data must, in addition to having a legal basis
always comply with the basic principles set out in Article 5 i
the Data Protection Regulation. Among other things, personal data may only be used
for specific, explicit and justified purposes (the principle of
purpose limitation) and no more personal data may be processed than
necessary for the purposes (data minimization principle). Of Article 32

follows that the data controller has to take appropriate technical and
organizational measures for personal data to ensure a
a level of safety appropriate to the risk to natural persons
rights and freedoms. Furthermore, the person responsible for personal data, according to

Article 32 (4), take measures to ensure that each natural person performing
work under the supervision of the data controller, and who may
access to personal data, only processes these on instructions from it
personal data controller.

The Data Inspectorate's assessment of the publication

The Data Inspectorate assesses that the publication of a private person
correspondence to an authority has gone beyond a conceivable purpose of
publish parts of the current case on the web (to provide the public with insight into
municipal activities). Thus, there has been nothing special,
expressly stated and justified purpose of the publication of the relevant
personal data. Furthermore, there has been no legal basis for that
publish the personal data and the publication has not been covered by anything
exceptions to the ban on the processing of sensitive personal data.

Social security numbers have been published without the conditions set out in ch. § 10
the Data Protection Act have been complied with.

The Health and Medical Care Board has only worked with oral
instructions to the employees who were responsible for publishing the board'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 has failed in the instructions to those who work under the board
oversight. This means that the board has not taken appropriate action
organizational security measures to protect against unauthorized publication of
personal information on the web.

The Data Inspectorate has in a number of decisions about 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 should be used by staff and should

determine when personal data may be published, who should do it

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

apply on 24 May 2018. The Data Inspectorate was the supervisory authority according to PuL until

The Data Protection Ordinance began to apply on 25 May 2018.

the assessment, how long the data should be stored on the web, work routine for

masking of sensitive or classified information, handling of linked

documents and an indication of who is responsible for publication and

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

to ensure that staff receive adequate 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 the person who publishes personal data on

the website does this in accordance with its instructions

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.

Sufficient measures have not been taken to ensure that those who

publishes personal data under the supervision of the board does so in accordance

with the board's instructions for publication.

The Data Inspectorate therefore states that the Health and Medical Care Board in

Örebro County Region has violated Articles 5, 6, 9 and 32 of

the Data Protection Ordinance, and ch. Section 10 of the Data Protection Act.

Choice of intervention

The Data Inspectorate has found that the board has published sensitive personal information and social security number on Region Örebro County's website and that the board lacks written routines for web publishing. The publication which 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 board has considered personal data in breach of the principles of purpose limitation and data minimization in Article 5 of the Data Protection Regulation, the provision on legal treatment in Article 6 and the ban on the treatment of sensitive personal data in Article 9. The publication of social security numbers does not comply the conditions in ch. Section 10 of the Data Protection Act and is therefore contrary to it the provision.

Article 58 of the Data Protection Regulation lists all of the Data Inspectorate powers. The Data Inspectorate has in case 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 available under Article 58 (2) (a) to (j), including reprimand, injunction and penalty fees.

It follows from Article 58 (2) of the Data Protection Ordinance that the Data Inspectorate in in accordance with Article 83 shall impose penalty charges in addition to or in lieu of other corrective measures referred to in Article 58 (2), the circumstances of each individual case. If it is a question of a smaller

infringement, the supervisory authority may, in accordance with recital 148 i
the Data Protection Regulation, issue a reprimand instead of imposing one
penalty fee.

A penalty fee shall be paid

The Data Inspectorate has assessed that the board has violated Articles 5, 6, 9
and 32 in the Data Protection Ordinance and Chapter 3. Section 10 of the Data Protection Act, adopted
on the basis of Article 87 of the Data Protection Regulation. These articles are covered
of Articles 83.4 and 83.5. In the event of a violation of these shall
the supervisory authority consider imposing administrative penalty fees
in addition to, or instead of, other corrective actions.

The Data Inspectorate assesses that this is not a minor violation.
This is against the background that the personal data that was published was sensitive
and touched a patient. Furthermore, the person could not reasonably expect that
his correspondence was made available to a large circle. In addition, var
the personal data was published for a long time without it being discovered by
the board. There is no reason to reimburse the penalty fee with anyone else
Corrective Action. The Health and Medical Care Board must thus be imposed on one
administrative penalty fee.

Determination of the amount of the sanction

According to Article 83 (1) of the Data Protection Regulation, each supervisory authority shall:
ensure that the imposition of administrative penalty fees in each individual
cases are 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
infringements referred to in Article 83 (4) of the Data Protection Regulation and at most
SEK 10,000,000 for infringements referred to in Article 83 (5). Violations of

Articles 5, 6, 9 and 3 Section 10 of the Data Protection Act (adopted on the basis of

Article 87) are subject to the higher penalty fees referred to in Article 83 (5) and

7 (10)

infringements of Article 32 are covered by the lower maximum amount referred to in Article

83.4.

Article 83 (2) of the Data Protection Regulation sets out factors to be taken into account in

determining the amount of the penalty fee. These factors include a)

the nature, severity and duration of the infringement; (b) the infringement

committed intentionally or through negligence; (c) the measures taken by it

personal data controllers have taken to alleviate the damage 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 infringement;

manner in which the infringement came to the attention of the supervisory authority, in particular

whether and to what extent the person responsible for personal data reported

the infringement.

The Data Inspectorate's assessment of the size of the penalty fee is taken into account

taken to the following.

The violation has concerned sensitive personal data regarding a person in

dependency for which the publication of the data may have been obtained

serious consequences. Furthermore, the information has been published openly

the region's website for a long time. That there was a lack of appropriate technical

and organizational measures to ensure such personal data do not

published poses a risk that similar events will occur again.

The lack of appropriate security measures is reflected in the fact that the board does not himself discovered the incorrect publication. However, the publication has not intentionally and there is no indication that more than one person in the reality would have been affected by incorrect publications of sensitive personal data. The board will be added to this as soon as it becomes aware if the event has acted by deleting the published document, inform the data subject and inform the staff concerned and that work has begun on developing written routines. The Data Inspectorate also notes that the region has made a personal data incident report on behalf of the board to the Data Inspectorate and followed the regulations that exists in that respect.

The publication of personal data on the board's open website refers to one and the same conduct and includes infringement of Articles 5, 6 and 9 of the Data Protection Ordinance and Chapter 3. Section 10 of the Data Protection Act.

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

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

refers to the violation of Article 32 of the Data Protection Regulation.

Order for further organizational measures

Pursuant to Article 58 (2) (d), the Data Inspectorate has the power to impose a personal data controller to ensure that a processing takes place in accordance with the provisions of the Data Protection Regulation. It is clear from Article 58 (2) that administrative penalty fees can be combined with injunctions.

The Health and Medical Care Board has not taken sufficient organizational steps 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 drawing up written instructions and ensuring that the person publishes personal information on the website does so in accordance with the instructions.

The Health and Medical Care Board in Örebro County Region must therefore be ordered to establish written instructions and establish procedures to ensure that who publish personal data on open websites do so accordingly with the instructions.

This decision was made by the Director General Lena Lindgren Schelin after presentation by [lawyer] Elin Hallström. At the final processing also has General Counsel Hans-Olof Lindblom, Unit Manager Malin Blixt and unit manager Katarina Tullstedt participated. IT security specialist Magnus Bergström has participated in the assessments concerning information security.

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

Appendix

How to pay penalty fee

Copy for information to:

The Data Protection Officer

How to appeal

If you want to appeal the decision, you must write to the Data Inspectorate. Enter i

the letter which decision you are appealing and the change you are requesting.

The appeal must have been received by the Data Inspectorate no later than three weeks from

the day the decision was announced. If the appeal has been received in due time

the Data Inspectorate forwards it to the Administrative Court in Stockholm

examination.

You can e-mail the appeal to the Data Inspectorate if it does not contain

any privacy-sensitive personal data or data that may be covered by

secrecy. The authority's contact information can be found on the first page of the decision.