Decision

Diary no

2020-04-28

DI-2019-10409

The State Service Center, SSC

The state service center's management of a

personal data incident - Supervision according to

data protection regulation

Table of Contents

The Swedish Data Protection Authority's decision..... 2

Statement of the supervisory matter 3

The State Service Center's tasks..... 4

Other things that came to light in the inspection..... 7

Justification of decision..... 7

Legal background..... 7

General about the responsibility for personal data processing.....7

Obligation to have a personal data processor agreement 8

Obligation to notify personal data controller.....8

Obligation to report to the Data Inspectorate..... ..9

Obligation to document personal data incidents 9

The Swedish Data Protection Authority's assessment..... 10

Distribution of roles and summary of the sequence of events 10

The notifications to the authorities were made too late 11

The notification to the Data Inspectorate was made too late 11

No valid personal data processing agreement 12

Shortcomings in the documentation as a personal data controller 13

Choice of intervention 14

Legal regulation 14

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

Penalty fees to be imposed 15

Personal data assistant agreement 15

Circumstances of importance for determining the amount of the penalty fee 16

Injunction due to deficiencies in documentation 17

Appendix..... 18

Copy for information 18

How to appeal..... 18

The Swedish Data Protection Authority's decision

The Data Inspectorate states that the State Service Center in its capacity of

personal data officer only notified on 20 August 2019

authorities responsible for personal data about a personal data incident which

the authority became aware of on 28 March 2019. This means that the State's

service center violated article 33.2 of the data protection regulation, then

the intelligence did not take place without unnecessary delay after the State's

service center became aware of the personal data incident.

The Data Inspection Authority decides with the support of ch. 6. Section 2 of the Data Protection Act and

articles 58.2 and 83 of the data protection regulation that the Statens service center shall

pay an administrative sanction fee of SEK 150,000 for the violation

of Article 33.2 of the Data Protection Regulation, that is, for the failure to

without undue delay notify the personal data controllers

the authorities about the personal data incident in question in the supervisory matter.

The Data Inspectorate states that the State Service Center in its capacity of

personal data controller only on 25 June 2019 until the Data Inspection came in

with a notification of a personal data incident that the authority received

knowledge of March 28, 2019. This means that the State Service Centre

violated article 33.1 of the data protection regulation, then notification of

the personal data incident did not take place within 72 hours after the State's

service center became aware of it.

Furthermore, the Statens service center as personal data controller does not

documented essential circumstances surrounding the personal data incident

and the corrective measures that have been taken and thereby violated Article 33.5

in the data protection regulation.

The Data Inspection Authority decides with the support of ch. 6. Section 2 of the Data Protection Act and

articles 58.2 and 83 of the data protection regulation that the Statens service center shall

pay an administrative sanction fee of SEK 50,000 for the violation

of Article 33.1 of the Data Protection Regulation, that is, for the failure to

report the personal data incident to the Swedish Data Protection Authority within 72 hours after

to have become aware of it.

The Swedish Data Protection Authority decides to instruct the Staten's Service Center with the support of Article 58.1 d of the

Data Protection Ordinance to:

1. Establish procedures for documentation of personal data incidents such as

makes it possible for the Swedish Data Protection Authority to check compliance with

Article 33 of the Data Protection Regulation. The routines must meet the requirements of

article 33.5 of the data protection regulation, which stipulates that it

personal data controller must document all

personal data incidents, including the circumstances surrounding

the personal data incident, its effects and the corrective measures

as taken, and thereafter

2. continuously check and ensure that the routines are followed.

The Data Inspectorate notes that the State's service center as personal data assistant and personal data manager at the time

of the inspection lacked

personal data processing agreement that complied with the requirements of Article 28.4

respectively Article 28.3 of the data protection regulation, but that the State's

service centers now have personal data processing agreements that meet

the regulation's requirements. In this case, the Swedish Data Protection Authority takes no further action

corrective action due to this initially established

lack.

Account of the supervisory matter

A notification of a personal data incident regarding personal data that

concerned personnel at the Statens service center (hereafter SSC) and who were treated in

the Primula system was submitted to the Data Inspectorate on 25 June 2019. According to

report, the incident was discovered on March 28, 2019. The Swedish Data Protection Authority received

also in, from 13 August 2019 until the supervision was initiated, 37

notifications of personal data incidents in Primula from authorities such as

SSC is personal data assistant for, i.e. personal data controller

agencies. Each of the authorities responsible for personal data received

knowledge of the incident through a notification from SSC. According to

the reports, the incident occurred from and including March 14

on 30 May 2019. One of the authorities responsible for personal data attached

to his notification the said notification from SSC, which was dated 12

August 2019.

The Swedish Data Protection Authority has started supervision with the aim of reviewing SSC's handling of

personal data incidents in the Primula system. The inspection began with a

letter to SSC on 18 September 2018 and followed up with the request for

completion on 5 November 2019 and 17 January 2020 respectively.

The State Service Center's tasks

SSC has essentially stated the following in response to the Data Inspectorate's questions.

On March 28, 2019, SSC received a notification from an employee of the same authority via the data protection officer of an

authority responsible for personal data

(hereinafter "the notifier") that it was possible to access personal data which

belonged to other authorities responsible for personal data. An internal incident report was drawn up by SSC within twelve

hours of this time. That bug

which was assumed to be the source of the problem was considered fixed on March 29, 2019.

However, it turned out that the bug was not solved or that new bugs appeared.

The complainant pointed this out to the SSC during April. SSC failed to recreate

the incident as described by the complainant. May 21, 2019 left

the notifier additional information about how the bug appeared and how it came to light

also that the notifier has taken additional programming measures in Primula.

SSC reported the matter to the personal data officer EVRY, as on 3 June

announced that the matter was resolved. SSC reported the complainant to the police on 24 May 2019 because according to SSC it was clear that he himself developed and executed code in Primula in order to prepare access to data.

On August 12, 2019, SSC sent a notification re the personal data incident to the 47 authorities responsible for personal data who made use of Primula. A supplementary dispatch to the same authorities was made on August 29, 2019.

About 282,000 registrants, of which 1,800 were employed by SSC, were affected by the personal data incident. The following categories of personal data

covered: social security number, name, information on gender, information on protected address information (but not the protected data), economic or financial information (documents for calculating the correct tax such as tax table, tax column, equalization, percentage tax, country of citizenship and work and so on), period of employment, place of duty, work permit, key person, calculated NOR, note about next of kin (however, no information about who it is relatives are).

Regarding the degree of sensitivity of the data, according to SSC information about social security numbers are partly considered worthy of protection in themselves, and partly regulated by strong confidentiality according to ch. 39 Section 3 of the Publicity and Confidentiality Act (2009:400), OSL. The latter secrecy applies to nine of the authorities that used it Primula. Information that someone has protected address information may be covered of confidentiality according to ch. 21 § 3 and ch. 39 Section 3 first paragraph OSL, confidentiality is then extra weak or weak. SSC's assessment was therefore that some of

the personal data was subject to confidentiality and was of a privacy-sensitive nature.

The reason SSC delayed notifying was that SSC wanted to

confirmed if and how the incident occurred before the relevant authorities

was notified, which according to SSC is a prerequisite for being considered to have

knowledge/knowledge of the incident according to Article 33.2. The same reason was behind that

SSC, in its capacity as data controller, delayed reporting

the personal data incident to the Data Inspectorate. It was also stated in the report

about the personal data incident that it was still unclear how the unauthorized

the access actually looked like and whether unauthorized persons had access to

personal data for which SSC was the data controller, which it had not

could be confirmed at the time of notification.

The SSC perceived the responses provided by the system supplier, EVRY, as

vague Shortly after the incident, SSC asked the system provider about users

could access personal data of persons outside their own authority.

After that, SSC held recurring follow-up meetings and continued to ask

same question without getting a concrete answer from the system supplier. SSC got

nor an answer after the authority asked the question by email. After summer

SSC deemed it necessary to notify those concerned

the authorities, although the data (of the incident) still did not have

confirmed. At that time, the SSC also did not consider that there was any concern

to expose ongoing security flaws in the system by leaving

notification of the suspected incident.

It became clear relatively quickly after the report came in to SSC that there was

security flaws in Primula, but not necessarily that there has been one

personal data incident, except for the authority that reported the deficiency. The

On 20 August 2019, SSC received confirmation that it was possible to take part

personal data at other authorities for which SSC was personal data assistant

at. SSC has stated that the service center did not adequately investigate the incident

urgently and that the lack of clear and documented routines to

dealing with these issues in a coordinated manner has contributed to the delay with

to notify the relevant authorities.

SSC has a personal data processing agreement with EVRY which was made in the meantime

for the Personal Data Act (1998:204), PUL. Already before

the data protection regulation's entry into force, however, SSC has applied for a change in

existing PUB agreement to replace this with one that follows

the data protection regulation's terminology and form requirements in general.

SSC has documented the personal data incident through a police report, SSC's

notification to the Data Inspectorate, the notifications to them

the authorities responsible for personal data, the incident report which

was established and the communication with the notifier who discovered and

exploited the security hole. The documentation is kept in three different diaries

cases, of which the intelligence, the incident report and the communication

with the notifier is a separate matter.

After final communication, SSC has made the following points of view.

The personal data processor EVRY has contractually committed to deliver

a service that is compatible with current legislation. As an expression of that

agreed the requirement that the service must be compatible with current legislation has

Before the entry into force of the data protection regulation, SSC asked a number of questions

EVRY on how the new requirements resulting from the data protection regulation are handled

and secured in Primula. EVRY has both provided answers and changed functionality in the service, as a consequence of the new requirements. The commitments contained in it then the current PUB agreement, together with other security requirements and contractual commitments, meant a perfectly adequate regulation in terms of material protection and the processing of personal data. It happened the personal data incident, and the deficiencies that subsequently existed in the handling, was not a consequence of the then current personal data processor agreement or

other agreed commitments. However, SSC now has an updated one personal data processing agreement with EVRY regarding Primula.

The Data Inspectorate's form for reporting personal data incidents has used by SSC. It would be remarkable if the Data Inspectorate at its control of compliance with Article 33 requires further documentation than the basis according to which personal data controllers The Swedish Data Protection Authority's own documents are obliged to report.

Other things that emerged in the inspection

The Swedish Data Protection Authority has taken note of the incident report that SSC drew up connection with notification from a person to an authority on March 28, 2019. I the report describes how the person who reported the incident could see among different social security number for all employees of certain authorities. The report further states that the incident based on damages, costs and consequences is that view as very serious “when sensitive data became available to users who should not have access to these”.

The Swedish Data Protection Authority has noted that SSC in the notification to the authorities

on 12 August 2019 states that the SSC has deemed it necessary to ensure

that the necessary security measures have been taken before such notification

was left. This is because "the information concerns a number of authorities which

thereby gaining knowledge of each other's security flaws".

Datainspektionen has requested the police report that SSC made on 24 May

2019. From the police report it appears that SSC reported that a person who was employed

at one of the authorities that use SSC for their payroll processing, at two different times

occasions illegally entered the system and thus gained access

information belonging to other authorities and that the information consisted of

personal data and "payroll data".

Justification of decisions

Legal background

General about responsibility for personal data processing

A personal data controller is responsible for compliance

the provisions of the data protection regulation when processing personal data,

and to ensure that hired personal data processors comply

data protection regulation when they process personal data. IN

data protection regulation, this is clear from the fact that its provisions essentially

addresses the personal data controller, that he is responsible for according to Article 24

to implement technical and organizational measures to ensure and

be able to demonstrate that the processing of personal data takes place in accordance with

the data protection regulation and that according to article 28 it must only engage

personal data assistants who provide sufficient guarantees to carry out

appropriate such measures.

A data controller, including sub-processors, is responsible for compliance

the provisions of the data protection regulation that are directly aimed at

personal data assistants, including Article 33.2. In addition, can

personal data assistants become liable for violations of

the data protection regulation which is a consequence of their failure to comply with it

instructions of the data controller.

Obligation to have a personal data processing agreement

According to Article 28.3 of the Data Protection Regulation, a personal data assistant must be provided

processing of personal data on behalf of the data controller

regulated by a personal data processor agreement (or other binding legal act).

The agreement must, among other things, prescribe an obligation for personal data assistants

to ensure that the obligations in Articles 32-36 of the Data Protection Regulation

is fulfilled, taking into account the type of treatment and the information that

the personal data assistant must be available.

Personal data assistants hired by personal data assistants, so-called

assistants, shall be imposed according to Article 28.4 of the data protection regulation

the same data protection obligations set out in the personal data processor agreement with the personal data controller. Above

all, the agreement must provide

sufficient guarantees that the subcontractor will carry out appropriate technical

and organizational measures in such a way that the processing meets

the requirements of the data protection regulation. The obligations must be imposed through an agreement

(or other binding legal act).

Obligation to notify the controller of personal data

Personal data assistants must notify the personal data controller without delay after the assistant becomes aware that a

personal data incident has

took place, see article 33.2 of the data protection regulation. The personal data assistant shall

thus not make any probability assessment regarding the risks for them

registered rights and freedoms. It is the personal data controller who

must assess whether the personal data incident is such that it must be reported to

the supervisory authority. In order for the personal data controller to be able to fulfill

its notification obligation requires that the personal data assistant quickly

notifies the person in charge.

Obligation to report to the Data Protection Authority

It is clear from article 33.1 of the data protection regulation that the person responsible for personal data in the event of a

personal data incident must report the incident to

the supervisory authority without undue delay and, if possible, not later

than 72 hours after becoming aware of it. If it is unlikely that

the personal data incident poses a risk to the rights of natural persons

and freedoms it does not need to be reported. If and to the extent it is not

possible to provide the information at the same time, receives the information

provided in installments without unnecessary further delay, see Article 33.4 i

data protection regulation.

According to the Article 29 Group's guidance WP250, in the event of a potential incident, the data controller may carry out a

brief investigation to

determine whether an incident has actually taken place. During this

investigation period, the personal data controller cannot be considered to have received

"knowledge" of the incident. In most cases, according to the same guidance,

risk assessment and notification to the regulatory authority is completed as soon as possible

possible after the initial warning/suspicion that a

security incident has taken place which may involve personal data. Only in

in exceptional cases this should take longer. 1

Obligation to document personal data incidents

According to article 33.5 of the data protection regulation, the personal data controller must

document all personal data incidents, including the circumstances

about the personal data incident, its effects and the corrective measures

as taken. The documentation must make it possible for

the supervisory authority to check compliance with Article 33 i

data protection regulation.

Article 29 - Working Party on Data Protection, WP250rev.01; Guidelines on notification of

personal data incidents according to Regulation (EU) 2016/679; adopted on 3 October 2017;

last reviewed and adopted on February 6, 2018; adopted by the EDPB during the first

the plenary session on 25 May 2018; pp. 11–12. The working group was established according to Article 29 i

1

directive 95/46/EC and was an independent EU advisory body in matters relating to data protection

and integrity.

The documentation obligation in Article 33.5 is linked to

the liability in Article 5.2 of the Data Protection Regulation, that is to say that

the personal data controller must be responsible for and be able to demonstrate that they

the basic principles of data protection are complied with. There is also one

connection between article 33.5 and article 24 of the data protection regulation. The

the latter provision means that the person in charge of personal data must take

technical and organizational measures to ensure and be able to demonstrate that
it performs personal data processing in accordance with
the provisions of the data protection regulation.2

The Swedish Data Protection Authority's assessment

Role distribution and summary of the course of events

SSC has regarding the violations of the data protection regulation like this
decisions relate to acting in different roles, as personal data controller and
personal data assistant. SSC has acted in the capacity of personal data processor
against 47 authorities responsible for personal data which, through
the connection to SSC, uses the system Primula for handling of
personal data about its staff. However, SSC has acted in the capacity of
personal data controller when processing personal data about their own
the authority's staff in the same system. SSC has hired the company EVRY as
personal data assistant for the operation of the system Primula. EVRY thus has
been personal data assistant for the processing of both personal data about
employees of the 47 authorities responsible for personal data which
personal data about employees of SSC.

An incident occurred on March 14, 2019, and on March 28, 2019, SSC received
a notification of the incident from the notifier. The notifier believed that the
could see personal data from other authorities than their own in Primula. One
incident report was prepared by SSC on March 28, 2019. After reporting
supplemented with additional information from the notifier on 21 May 2019
SSC drew up a police report against him on 24 May 2019.

As a personal data controller, SSC notified the above described
personal data incident to the Swedish Data Protection Authority on 25 June 2019. Report
referred to unauthorized access to personal data about the authority's own

staff.

2

WP250, rev01, p. 28.

In its capacity as data controller, SSC notified the 47

the authorities responsible for personal data on 12 August 2019.

On August 20, 2019, EVRY confirmed to SSC that the personal data incident

meant that it was possible for employees of any of the agencies that

used Primula to access personal data from the others

authorities that used the system.

The notifications to the authorities were made too late

The Norwegian Data Inspection Authority states that it took almost five months from that

that the incident was discovered on March 28, 2019 until SSC notified them

the authorities responsible for personal data on 12 August 2019. It is significant

more time than may be considered required for a shorter examination to

acquire knowledge that a personal data incident has occurred. To this

will SSC made a notification for its own part about six weeks before

the customer authorities were notified. It is clear that the SSC did not know more about

how the incident affected the personal data of the own staff than how

it affected employees of the authorities responsible for personal data. Major

knowledge therefore cannot justify that SSC did not send intelligence to them

the authorities in charge of personal data despite the fact that they made a report to

The Swedish Data Protection Authority for its own part.

The Data Protection Regulation requires that the person in charge of personal data be

notified without undue delay so that it may take the measures which

is needed due to an incident that has occurred. The Swedish Data Protection Authority assesses

that SSC had sufficient knowledge to be obliged to inform them

the authorities responsible for personal data already after the first notification from

a data protection officer at one of the authorities. It was then missing according to

Datainspektionen's assessment reason for SSC to wait

the notification to the authorities responsible for personal data in order to

"ensure that the necessary safety measures have been taken".

The Swedish Data Protection Authority states that SSC by only having on 20 August 2019

notified the authorities responsible for personal data have violated article

33.2 of the data protection regulation.

The notification to the Swedish Data Protection Authority was made too late

The Swedish Data Protection Authority notes that it took almost three months from the time that

the incident came to SSC's attention on March 28, 2019 to the extent that SSC

submitted a report about the incident to the Data Inspectorate on 25 June

2019. This far exceeds the 72 hour time limit stated in Article

32.1 of the data protection regulation. It is also significantly more time than can

is considered required for a shorter examination to acquire knowledge that

a personal data incident has occurred.

SSC has stated to the Swedish Data Protection Authority that they, in the sense referred to in

Article 33 of the Data Protection Regulation, became aware of the incident on 20

August 2019 when EVRY confirmed that personal data could be accessed between them

the authorities that used Primula. The Swedish Data Protection Authority has in this

regard taken note of SSC's actions both as a personal data controller and

as data controller because SSC acted on the same incident i

both roles.

The Data Inspectorate's assessment is that SSC must have known that a

personal data incident had occurred, in the sense that SSC believed

the information provided to the authority about the personal data incident

on 28 March 2019 and 21 May 2019. The clearest indication of this

is that what was stated in the report to the Police Authority on 24 May 2019 was

that a person has access to personal data belonging to other authorities. To

judging by the internal report, the SSC did not dispute the information about the incident when

it was established on March 28, 2019.

Datainspektionen states against the background of the above that SSC has

violated article 33.1 of the data protection regulation by not reporting

the personal data incident within 72 hours from the time of notification

entered SSC on March 28, 2019.

No valid personal data processing agreement

During the period 28 March 2019 to and including 20 August 2019, SSC had, i

property of a data processor, not a data processor agreement with

EVRY which corresponded to the requirements of what a personal data processing agreement should

contain according to article 28.4 of the data protection regulation. SSC in capacity of

personal data controller was missing during the same period one

personal data assistant agreement with EVRY that corresponded to the requirements of what one

personal data assistant agreement must contain according to Article 28.3.

As a personal data controller, SSC has to ensure that it
personal data processing carried out on behalf of the authority is covered by
a personal data processing agreement.
An agreement between personal data assistants must have a content that corresponds
the requirements in Article 28.3. It is clear from article 28.4, which stipulates that the agreement
above all must "give sufficient guarantees to carry out appropriate technical
and organizational measures in such a way that the processing meets
the requirements of this regulation". It is the personal data assistant who hires one
other assistant, in this case SSC, who will ensure that there is an agreement that
meets the specified requirements. This because the former
the personal data assistant is responsible for the processing of personal data vis-à-vis
the personal data controller for the assistants he has engaged.
The Swedish Data Protection Authority notes that SSC in its capacity as data controller
respectively in the capacity of personal data assistant violated articles 28.3 and
28.4 of the data protection regulation by having hired one
personal data assistant without stipulating in an agreement or other legal act
such obligations as required by Article 28 of the Data Protection Regulation.
Shortcomings in the documentation in the role of personal data controller
The Data Inspectorate states that the documentation of
the personal data incident brought in by SSC does not clarify how SSC
complied with the notification that came from the informant and that gave SSC
knowledge of the incident. It is not clear how the SSC attempts to recreate
the incident took place and what grounds there were to question the information which
submitted by the notifier. Thus, the parts of the surrounding circumstances are missing
the personal data incident required to be able to demonstrate why the incident did not
reported within 72 hours. It is also not clear from the documentation what

SSC has done to get answers to the questions about the incident that SSC stated that the authority had. There is no information about the circumstances surrounding the personal data incident that could have explained the delay with notification. Furthermore, the SSC has explained that the documentation of the personal data incident as far as SSC as personal data controller is concerned - in form of the police report, report to the Data Inspectorate, prepared incident report and communication with the user who notified the SSC, is in three matters in SSC's diary. The case with the most documentation – the notifications to the authorities, the incident report and the communication with the user, is in a matter relating to the SSC's role

as personal data assistant. The documentation does not show that it has been done to fulfill the obligation according to Article 33.5 of the Data Protection Regulation but appears to be motivated and ordered according to other principles.

A prerequisite for the Swedish Data Protection Authority to be able to follow up on a personal data incident based on the documentation is that it is aggregated and gives a fair picture of the course of events. The documentation has in it this case did not make it possible for the Swedish Data Protection Authority to check compliance with Article 33 of the Data Protection Regulation.

The Swedish Data Protection Authority notes that SSC in its capacity as data controller has violated Article 33.5 of the Data Protection Regulation by not document the personal data incident in a way that made it possible for the supervisory authority to check compliance with Article 33 i data protection regulation.

Choice of intervention

Legal regulation

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

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.

The Swedish Data Protection Authority has assessed above that SSC in the current processing of

personal data has violated articles 33 and 28 of the data protection regulation.

These articles are covered by article 83.4, which means that penalty fees which

main rule must be applied. It is a question of an authority. The penalty fee

can therefore according to ch. 6 Section 2 of the Data Protection Act (2018:218) is determined at most

SEK 5,000,000.

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.

In article 83.2 of the data protection regulation, all factors that must

taken into account when determining the size of the penalty fee. At the assessment
of the size of the penalty fee, account must be taken of, among other things, a)
the nature, severity and duration of the infringement, b) intent or
negligence, and g) the categories of personal data affected by
the violation.
Penalty fees shall be imposed
The personal data incidents that SSC did not notify the 47
the authorities responsible for personal data if personal data is covered in time
about 280,000 registered. The personal data that was at risk of being disclosed
included, among other things, social security numbers, information that people have been protected
address (but not the protected data itself) and information about
employment. It took almost five months before they
The authorities responsible for personal data were notified from the time SSC received
knowledge of the personal data incident. It is therefore not a question of less
violations and there is no reason to replace the penalty fee with one
reprimand.
The personal data incident that SSC in its capacity as data controller
not reported to the supervisory authority Datainspektionen in time covered
personal data of approximately 1,800 registered users. The personal data that
were at risk of being revealed covered, among other things, social security numbers, information that
persons have protected address and information about employment. It took some time
almost three months before SSC came in with another report
The Swedish Data Protection Authority from the time SSC became aware of the personal data incident.
The Swedish Data Protection Authority finds that it is not a question of a minor violation and
that there is no reason to replace the penalty fee with someone else
Corrective Action.

SSC shall therefore be subject to administrative penalty fees for these violations.

Personal data service agreement

The Swedish Data Protection Authority has also stated that SSC did not have personal data processing agreement that complied with the requirements of articles 28.3 and 28.4 of the data protection regulation. However, SSC has stated that SSC had

personal data processing agreements that were drawn up in accordance with the Personal Data Act, that work was underway to update the agreements and that SSC now has a personal data processing agreement with EVRY which complies with the requirements of the data protection regulation. Against that background the Data Inspectorate finds that in this case there are reasons not to impose one special penalty fee or other corrective action due to the deficiency that previously existed.

Circumstances of importance for determining the penalty fee size

The personal data incident affected approximately 280,000 employees at 47 authorities responsible for personal data as regards SSC's role as personal data assistant and approximately 1,800 employees at SSC in terms of SSC's role as personal data controller.

The Swedish Data Protection Authority has, when assessing the penalty fee that applies the failure to notify the personal data controllers in time authorities, judged that the delay is in clear conflict with the weight of personal data controllers quickly receiving information about incidents

personal data incidents so that they can take appropriate action.

That the information reaches out quickly is particularly important if

the personal data incident involves a high risk for natural persons

rights and freedoms, because the personal data controller must then

inform the data subjects without delay (see Article 34 i

data protection regulation). The Swedish Data Protection Authority notes that in this case

there has not been a question of a personal data incident that likely involved one

such high risk. The Swedish Data Protection Authority assesses that this causes the delay

can be assessed as less serious than it might otherwise have been

the case.

At the same time, the Data Inspectorate considers that the incident involved a large number

registered, that it concerned the authority's core business and that it has

took several months from the time the SSC became aware of it until the time the SSC

informed the authorities. These circumstances are aggravating. It will

it is also emphasized that there is a larger number of violations, through i

the basis the same wrongful act, because each of the 47 affected

the authorities would have been notified without undue delay.

Regarding the penalty fee for the failure to notify in time

the personal data incident to the supervisory authority, that is to

Datainspektionen, this omission covered a smaller number

registered than the failure to notify the personal data controllers

authorities. An aggravating circumstance is also in this case that it

It took several months before SSC came in with another report

The Swedish Data Protection Authority.

As regards the nature of the personal data, the Swedish Data Protection Authority does not

reason to adopt a position other than SSC's regarding

the protection value of the personal data, i.e. that some of them were covered by

confidentiality and were privacy sensitive.

Regarding the delays in reporting and informing about the incident

done with intent or through negligence, the Data Inspectorate finds that SSC has

had an intention for the delays. The investigation shows that SSC, in it

meaning referred to in Article 33 of the Data Protection Regulation, had knowledge of

that a personal data incident occurred that involved both SSC's employees

as employees of the authorities responsible for personal data. This has

revealed partly through the internal personal data incident report which

was established on 28 March 2019, partly through the police report that SSC made

on 24 May 2019. Despite being aware of the incident, SSC has not reported it to

The Swedish Data Protection Authority in time or notified the authorities without authorization

delay. The provisions of Article 33 of the Data Protection Regulation are clear

as regards the time aspect and it moves, under the circumstances which

found out in the supervision, not about an excusable error of judgement.

The Swedish Data Protection Authority decides based on an overall assessment that the SSC shall

pay an administrative sanction fee of SEK 150,000 for the omission

to notify the authorities responsible for personal data

the personal data incident without undue delay and that SSC shall pay a

administrative sanction fee of SEK 50,000 for failure to report

the personal data incident to the Swedish Data Protection Authority without undue delay.

The amounts are intended to be effective, proportionate and dissuasive.

Injunction due to deficiencies in documentation

That the personal data incident was not documented in accordance with

the criteria in Article 33(5) have not constituted a minor infringement because

the documentation has not been able to be used by the Data Inspectorate to

check compliance with Article 33. In an examination in accordance with

article 83.2 a) however, the Data Inspectorate considers that the documentation nevertheless

has not been deficient to such an extent as to warrant the imposition of one

penalty fee. A penalty fee also does not appear to be proportionate.

However, SSC, in its capacity as data controller, must be ordered to

establish procedures for the documentation of personal data incidents that do so

possible for the Data Inspectorate to check compliance with Article 33 and

continue to check and ensure that these procedures are followed. The routines must

at least respond to the requirements of Article 33.5 of the Data Protection Regulation, which

stipulates that the data controller shall document all

personal data incidents, including the circumstances surrounding

the personal data incident, its effects and the corrective measures that

taken.

This decision has been made by the director general Lena Lindgren Schelin after

presentation by lawyer Elin Hallström. At the final processing has

also chief legal officer Hans-Olof Lindblom, unit manager Malin Blixt and

unit manager Katarina Tullstedt participated. IT security specialist Johan

Ma has participated in the assessments relating to information security.

Lena Lindgren Schelin, 2020-04-28 (This is an electronic signature)

Appendix

How to pay penalty fee

Copy for the attention of:

Data Protection Officer for the Norwegian Service Center

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.