Decision

Diarienr

2020-04-28

DI-2019-10409

Statens Servicecenter, SSC

The State Service Center's handling of a

personal data incident - Supervision according to

the Data Protection Regulation

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

The Data Inspectorate's decision

The Data Inspectorate finds that the State Service Center in its capacity as personal data assistant only on 20 August 2019 informed authorities responsible for personal data in the event of a personal data incident which the authority became aware of on March 28, 2019. This means that the State service center violated Article 33 (2) of the Data Protection Regulation, then the notifications did not take place without undue delay after the State service center gained knowledge of the personal data incident.

The Data Inspectorate decides on the basis of ch. Section 2 of the Data Protection Act and Articles 58 (2) and 83 of the Data Protection Ordinance that the State Service Center shall

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

of Article 33 (2) of the Data Protection Regulation, ie for failure to:

inform the data controllers without undue delay

the authorities of the personal data incident in question in the supervisory case.

The Data Inspectorate finds that the State Service Center in its capacity as

personal data manager only on 25 June 2019 to the Data Inspectorate came in

with a report of a personal data incident received by the authority

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

violated Article 33 (1) of the Data Protection Regulation, when notifying

the personal data incident did not occur within 72 hours after the State

service center got to know about it.

Furthermore, the State Service Center, as the person responsible for personal data, does not

documented significant circumstances surrounding the personal data incident

and the corrective measures taken, thereby infringing Article 33 (5)

in the Data Protection Regulation.

The Data Inspectorate decides on the basis of ch. Section 2 of the Data Protection Act and

Articles 58 (2) and 83 of the Data Protection Ordinance that the State Service Center shall

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

of Article 33 (1) of the Data Protection Regulation, ie for failure to:

report the personal data incident to the Data Inspectorate within 72 hours after

to have become aware of it.

The Data Inspectorate decides, on the basis of Article 58 (1) (d) of the Data Protection Ordinance, to order the State Service

Center to:

Establish routines for documentation of personal data incidents such as

enables the Data Inspectorate to check compliance with

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

Article 33 (5) of the Data Protection Regulation, which provides that it

the person responsible for personal data must document everyone

personal data incidents, including the circumstances surrounding

the personal data incident, its effects and the corrective actions

taken, and thereafter

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

The Data Inspectorate states that the State Service Center, as the personal data assistant and the person responsible for

personal data at the time of the inspection, lacked

personal data assistant agreements that complied with the requirements of Article 28 (4)

respectively Article 28 (3) of the Data Protection Ordinance, but that the State

service center now has personal data assistant agreements that comply

requirements of the Regulation. In this case, the Data Inspectorate takes no further action

corrective action in connection with this initially stated

lack.

Report on the supervisory matter

A report of a personal data incident regarding personal data such as

concerned staff at the State Service Center (hereinafter SSC) and who were treated in

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

The incident was discovered on March 28, 2019. The Data Inspectorate received

also in, from 13 August 2019 until the start of supervision, 37

reports of personal data incidents in Primula from authorities such as

SSC is the personal data assistant for, ie the person responsible for personal data

authorities. Each of the authorities responsible for personal data received

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

The incident occurred from March 14 through

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

to the notification mentioned notification from SSC, which was dated the 12th

August 2019.

The Data Inspectorate has initiated supervision in order to examine SSC's handling of

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

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

completion on 5 November 2019 and 17 January 2020 respectively.

Tasks of the State Service Center

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

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

authority responsible for personal data.

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

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

hours from this time. The bug

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

It turned out, however, that the bug was not resolved or that new bugs had arisen.

The complainant pointed this out to SSC in April. SSC failed to recreate

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

the notifier further information on how the bug appeared and it emerged

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

SSC reported the matter to the personal data assistant EVRY, as of 3 June

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

On August 12, 2019, SSC sent a notification the personal data incident to the 47 authorities responsible for personal data who used Primula. A supplementary mailing to the same authorities were made on August 29, 2019.

Approximately 282,000 registered persons, of whom 1,800 were employed by SSC, were affected by the personal data incident. The following categories of personal data

were included: social security number, name, information on gender, information on protected address information (except the protected information), economic or financial information (basis for calculating the correct tax such as tax table, tax column, adjustment, percentage tax, country of origin and country of employment and so on), period of employment, place of employment, work permit, key person, calculated NOR, note about relative (but not information about who it is relatives are).

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

the personal data was covered by confidentiality and was of a privacy-sensitive nature.

The reason SSC delayed notifying was that SSC wanted

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 of the incident according to Article 33 (2). The same reason was behind that

SSC in its capacity as personal data controller delayed reporting

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

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

access actually looked like and if unauthorized had access to

personal data for which SSC was responsible for personal data, which it did not have

could be confirmed at the time of notification.

SSC perceived the responses provided by the system vendor, EVRY, as

vaga. Shortly after the incident, the SSC asked the system vendor for users

could access personal data for persons outside their own authority.

Thereafter, the SSC held recurring follow-up meetings and continued to ask

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

nor an answer after the authority asked the question by e-mail. After summer

SSC considered it necessary to inform those concerned

authorities, although the data (on 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 notification came in to SSC that it existed

security flaws in Primula, but not necessarily that one has occurred

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

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

personal data at other authorities such as SSC was the personal data assistant

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

urgently and that the lack of clear and documented routines to

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

to inform the relevant authorities.

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

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

However, SSC has sought an amendment to the Data Protection Ordinance

existing PUB agreement to replace this with one that follows

the terminology of the Data Protection Ordinance and other formal requirements.

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

notification to the Data Inspectorate, the notifications to the

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 recorded in three different ones

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

with the notifier is a separate matter.

Following the final communication, SSC has made the following comments.

The personal data assistant EVRY has contractually agreed to deliver

a service that complies with applicable law. As an expression of that

agreed requirement that the service must be compatible with applicable law has

Prior to the entry into force of the Data Protection Ordinance, SSC posed a number of questions

EVRY on how the new requirements that follow from the Data Protection Regulation are handled

and secured in Primula. EVRY has provided answers as well as changed functionality in the service, as a result of the new requirements. The commitments that are in it then

regarding the PUB agreement, together with other security requirements and contractual obligations, entailed adequate regulation regarding the material protection

and the processing of personal data. It happened

the personal data incident, and the shortcomings that followed in the handling,

was not a consequence of the then valid personal data assistant agreement or

other agreed commitments. However, SSC now has an update

personal data assistant 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 documentation according to which personal data controllers

The Data Inspectorate's own documentation is required to report.

Other that has emerged in the supervision

The Data Inspectorate has read the incident report that SSC prepared in

in connection with a notification from a person to an authority on 28 March 2019. I

the report describes how the person who reported the incident could see among

another social security number for all employees of certain authorities. The report

further states that the incident based on damages, costs and consequences is that

see as very serious ”when sensitive information became available to users

who should not have access to these ”.

The Data Inspectorate has noted that SSC in the notification to the authorities

on 12 August 2019 states that 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 such as

thereby gaining knowledge of each other's safety deficiencies ”.

The Data Inspectorate has requested the police report that SSC made on 24 May

2019. The police report states that SSC reported that a person who was employed

at one of the authorities that hire SSC for their payroll management, at two different

occasions illegally entered the system and thus took part

information belonging to other authorities and that the information consisted of

personal data and "salary data".

Justification of decision

Legal background

General information about the responsibility for personal data processing

A personal data controller is responsible for ensuring that it complies

the provisions of the Data Protection Regulation in the processing of personal data,

and to ensure that hired personal data assistants follow

the Data Protection Regulation when processing personal data. IN

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

addressed to the data controller, that he is responsible in accordance with Article 24

to implement technical and organizational measures to ensure and

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

the Data Protection Regulation and that it should only use Article 28

personal data assistants who provide adequate guarantees to implement

appropriate such measures.

A personal data assistant, including sub-assistants, is responsible for following

the provisions of the Data Protection Regulation which are directly addressed

personal data assistants, including Article 33 (2). In addition, can

personal data assistants become liable for violations of

the Data Protection Regulation as a result of non-compliance

instructions of personal data controllers.

Obligation to have a personal data assistant agreement

Pursuant to Article 28 (3) of the Data Protection Regulation, a personal data assistant shall:

processing of personal data on behalf of the data controller

governed by a personal data assistant agreement (or other binding act).

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

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

fulfilled, taking into account the type of treatment and the information provided

the personal data assistant is available.

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

assistants, shall be imposed in accordance with Article 28 (4) of the Data Protection Regulation

the same obligations regarding data protection as specified in the personal data assistant agreement with the personal data

controller. Above all, the agreement must provide

adequate guarantees that the assistant will carry out appropriate technical

and organizational measures in such a way that the treatment meets

the requirements of the Data Protection Regulation. The obligations shall be imposed by an agreement

(or other binding act).

Obligation to notify personal data controllers

Personal data assistants shall without delay notify the personal data controller after the assistant has become aware that a

personal data incident has

occurred, see Article 33 (2) of the Data Protection Regulation. The personal data assistant shall

thus not making any probability assessment as to the risks to them

freedoms and rights were registered. It is the person responsible for personal data who

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

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

its duty to report is required to the personal data assistant quickly

informs the person responsible.

Obligation to report to the Data Inspectorate

It is stated in 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 learning of it. If it is unlikely to

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

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

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

provided in installments without undue delay, see Article 33 (4) (i)

the Data Protection Regulation.

According to the WP250 Guideline WP250, in the event of a potential incident, the controller may conduct a brief investigation

to

determine whether an incident has actually taken place. During this

examination period, the person responsible for personal data cannot be considered to have received

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

risk assessment and notification to the supervisory authority are completed as soon as

possible after the initial warning / suspicion that a

security incident has taken place which may include 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 controller shall:

document all personal data incidents, including the circumstances

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

taken. The documentation must make it possible for

the supervisory authority to monitor compliance with Article 33 i

the Data Protection Regulation.

Article 29 - Working Party on Data Protection, WP250rev.01; Guidelines for 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 in the first instance

plenary session on 25 May 2018; pp. 11–12. The working group was set up in accordance with Article 29 i

1

Directive 95/46 / EC and was an independent EU advisory body on data protection issues

and integrity.

The documentation obligation in Article 33 (5) is linked to

liability in Article 5 (2) of the Data Protection Regulation, ie

the person responsible for personal data must be responsible for and be able to show that they

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

link between Article 33 (5) and Article 24 of the Data Protection Regulation. The

the latter provision means that the person responsible for personal data must take

technical and organizational measures to ensure and be able to demonstrate that
it processes personal data in accordance with
the provisions of the Data Protection Regulation.2

The Data Inspectorate's assessment

Role distribution and summary of the course of events

SSC has regarding the violations of the Data Protection Regulation as this
decisions concern appearances in various roles, such as personal data controller and
personal data assistant. SSC has acted as a personal data assistant
vis-à-vis 47 authorities responsible for personal data which, through
connection to the SSC, uses the Primula system for handling
personal information about their staff. However, the SSC has acted in its capacity as
person responsible for personal data in the processing of personal data about one's own
authority staff in the same system. SSC has hired the company EVRY as
personal data assistant for the operation of the Primula system. EVRY has thus
has been a personal data assistant for the processing of both personal data about
employees of the 47 authorities responsible for personal data who
personal information about employees at SSC.

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

In its capacity as personal data controller, SSC notified the person described above
the personal data incident to the Data Inspectorate on 25 June 2019. Notification
referred to unauthorized access to personal data about the authority's own

staff.

2

WP250, rev01, p. 28.

As a personal data assistant, 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 authorities

used Primula to access personal data of the others

authorities that used the system.

The notifications to the authorities were made too late

The Data Inspectorate states that it took almost five months from that

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

the authorities responsible for personal data on 12 August 2019. This 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 report for its own part about six weeks before

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

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

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

knowledge can therefore not justify that SSC did not send notifications to them

authorities responsible for personal data even though they made a notification to

The Data Inspectorate for its own part.

The Data Protection Ordinance requires that the person responsible for personal data become

notified without undue delay so that it can take the measures necessary

needed due to an incident that has occurred. The Data Inspectorate assesses

that the SSC had sufficient knowledge to be required 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

The Data Inspectorate's assessment is a 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 Data Inspectorate states that SSC by only on 20 August 2019 ha

notified the authorities responsible for personal data has violated the article

33.2 of the Data Protection Regulation.

The report to the Data Inspectorate was made too late

The Data Inspectorate states that it took almost three months from that

the incident came to SSC's notice on March 28, 2019 to the SSC

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

2019. This far exceeds the time limit of 72 hours specified in Article

32.1 of the Data Protection Regulation. It is also significantly more time than can be

is considered to be required for a shorter examination in order to acquire knowledge that

a personal data incident has occurred.

SSC has stated to the Data Inspectorate 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 among themselves

the authorities that used Primula. The Data Inspectorate has in this

with regard to SSC's actions both as personal data controller and

as a personal data assistant because SSC acted on the basis of the same incident in

both roles.

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

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

the information provided to the authority about the personal data incident

March 28, 2019 and May 21, 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 accessed personal data belonging to other authorities. To

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

it was established on March 28, 2019.

In light of the above, the Data Inspectorate states that SSC has

violated Article 33 (1) of the Data Protection Regulation by not notifying

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

entered the SSC on March 28, 2019.

No valid personal data assistant agreement

During the period March 28, 2019 through August 20, 2019, SSC, in

as a personal data assistant, not a personal data assistant agreement with

EVRY which corresponded to the requirements for what a personal data assistant agreement should be

contain in accordance with Article 28 (4) of the Data Protection Regulation. SSC as

during the same period, the data controller lacked one

personal data assistant agreement with EVRY which corresponded to the requirements for what one

personal data assistant agreements shall contain in accordance with Article 28 (3).

As the data controller, SSC has to ensure that it

personal data processing performed on behalf of the authority is covered by

a personal data assistant agreement.

An agreement between personal data assistants must have a content that corresponds

the requirements of Article 28.3. It is stated in Article 28 (4), which provides that the agreement

above all, “shall provide adequate guarantees to implement appropriate technical

and organizational measures in such a way that the treatment meets

the requirements of this Regulation ". It is the personal data assistant who hires one

another assistant, in this case SSC, who will ensure that there is an agreement that

meets the specified requirements. This is because the former

the personal data assistant is responsible for the processing of personal data vis-à-vis

the personal data controller for the sub-assistants he has hired.

The Data Inspectorate finds that SSC in its capacity as personal data controller

respectively, in his capacity as personal data assistant, violated Articles 28 (3) and

28.4 of the Data Protection Regulation by having engaged a

personal data assistant without prescribing in an agreement or other legal act

obligations required by Article 28 of the Data Protection Regulation.

Deficiencies in the documentation in the role of personal data controller

The Data Inspectorate finds that the documentation of

the personal data incident that SSC came in with does not clarify how SSC

responded to the notification that came from the notifier and that gave SSC

knowledge of the incident. It is not clear how SSC's attempt to recreate

the incident took place and what were the reasons for questioning the information as

the notifier has left. Thus, those parts of the surrounding circumstances are missing

the personal data incident required to be able to show why the incident did not

was notified 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 it the personal data incident which could have explained the delay with notification. Furthermore, SSC has stated that the documentation of the personal data incident as far as SSC as personal data controller is concerned - in form of police report, report to the Data Inspectorate, prepared incident report and communication with the user who notified SSC, are in three cases in SSC's diary. The case that has the most documentation - the notifications to the authorities, the incident report and the communication with the user, is in a case concerning SSC's role

as a personal data assistant. The documentation does not show that it has been done to fulfill the obligation under Article 33 (5) of the Data Protection Regulation but appears to be motivated and arranged according to other principles.

A prerequisite for the Data Inspectorate to be able to follow one up personal data incident based on the documentation is that it is collected and gives a true picture of the course of events. The documentation has in it in this case not made it possible for the Data Inspectorate to check compliance with Article 33 of the Data Protection Regulation.

The Data Inspectorate finds that SSC in its capacity as personal data controller has infringed 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 monitor compliance with Article 33 i the Data Protection Regulation.

Choice of intervention

Legal regulation

Article 58 of the Data Protection Regulation lists all of the Data Inspectorate

powers. The Data Inspectorate has in case of violations of

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.

The Data Inspectorate has above assessed that SSC in the current treatments 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 such as

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

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

5,000,000 kronor.

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.

Article 83 (2) of the Data Protection Regulation sets out all the factors that must:

taken into account when determining the size of the penalty fee. In the assessment

of the size of the penalty fee, account shall be taken of, among other things:

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

negligence, and (g) the categories of personal data affected by

the infringement.

Penalty fees must be imposed

The personal data incidents that SSC did not notify the 47

the authorities responsible for personal data if in time included personal data

about 280,000 registered. Personal data that risked being disclosed

included, among other things, social security numbers, information that persons have been protected

address (but not the protected data per se) and details of

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 thus not a question of less

infringements and there is no reason to reimburse the penalty fee with one

reprimand.

The personal data incident as SSC in its capacity as personal data controller

did not report to the supervisory authority the Data Inspectorate in time covered

personal data of about 1,800 registered. The personal data as

at risk of being disclosed included, among other things, social security numbers, information that

persons have a protected address and employment information. It took some time

almost three months before SSC came in with another application

The Data Inspectorate from the time SSC became aware of the personal data incident.

The Data Inspectorate finds that this is not a minor violation and

that there is no reason to reimburse the penalty fee with someone else

Corrective Action.

SSC must therefore be subject to administrative sanction fees for these

violations.

Personal data assistant agreement

The Data Inspectorate has also found that SSC did not

personal data assistant agreements that complied with the requirements of Articles 28 (3)

and 28.4 of the Data Protection Regulation. However, the SSC has stated that the SSC had

personal data assistant agreements that were established in accordance with

the Personal Data Act, that work was in progress to update the agreements and that

SSC now has a personal data assistant agreement with EVRY as

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 apply one

special penalty fee or other corrective action due to

the shortcoming that previously existed.

Circumstances relevant to determining the penalty fee

size

The personal data incident affected approximately 280,000 employees at 47

authorities responsible for personal data with regard to SSC's role as

personal data assistant and approximately 1,800 employees at SSC with regard to SSC's role

as personal data controller.

The Data Inspectorate has, in assessing the penalty fee that applies

the failure to notify the data controllers in time

authorities, judged that the delay is in clear conflict with the weight

that the data controllers quickly receive information about what happened

personal data incidents so that they can take appropriate action.

That the information reaches out quickly is especially important if

The personal data incident involves a high risk for natural persons

rights and freedoms, as the person responsible for personal data shall then

inform the data subjects without delay (see Article 34 i

the Data Protection Regulation). The Data Inspectorate notes that in this case

has not been a personal data incident that probably involved one

such a high risk. The Data Inspectorate assesses that this causes the delay

can be judged to be less serious than could 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 core business of the authority and that it has

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

informed the authorities. These circumstances are aggravating. It will

It is also emphasized that this is a large number of infringements, by i

basically the same wrongdoing, as each of the 47 affected

the authorities would have been notified without undue delay.

As for the penalty fee for failure to report in time

the personal data incident to the supervisory authority, ie to

The Data Inspectorate, this omission included a small number

registered than the failure to notify the data controllers

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

it took several months before SSC came in with another application

The Data Inspectorate.

As regards the nature of the personal data, the Data Inspectorate does not have
reason to adopt a position other than SSC with regard to
the protection value of personal data, ie some of them were covered by
confidentiality and were sensitive to privacy.

As for the delays in reporting and notifying the incident
done intentionally or through negligence, the Data Inspectorate finds that SSC has
had intent to delay. The investigation shows that SSC, in the
within the meaning of Article 33 of the Data Protection Regulation
that a personal data incident has occurred that affected both SSC's employees
as employees of the authorities responsible for personal data. This has
appeared partly through the internal personal data incident report which
was established on March 28, 2019, partly through the police report made by SSC
on May 24, 2019. Despite knowing about the incident, SSC has not reported it to
The Data Inspectorate on time or notified the authorities without unauthorized use
delay. The provisions of Article 33 of the Data Protection Regulation are clear
in terms of the time aspect and it moves, in the circumstances that
appeared in the supervision, not about an excusable error of assessment.

The Data Inspectorate decides on the basis of an overall assessment that SSC should
pay an administrative penalty fee of SEK 150,000 for the omission
to inform the authorities responsible for personal data
the personal data incident without undue delay and that the SSC must pay one
administrative sanction fee of SEK 50,000 for failure to report
the personal data incident to the Data Inspectorate without undue delay.

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

Order due to deficiencies in documentation

That the personal data incident was not documented in accordance with

the criteria set out in Article 33 (5) did not constitute a minor infringement because

the documentation could not 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 that it is justified to impose one

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

On the other hand, SSC, in its capacity as personal data controller, shall be ordered to:

establish routines for documentation of personal data incidents that do so

enable the Data Inspectorate to check compliance with Article 33 and

In the future, check and ensure that these routines are followed. The routines should

at least comply with the requirements of Article 33 (5) of the Data Protection Regulation, which

prescribes that the person responsible for personal data must document everyone

personal data incidents, including the circumstances surrounding

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

taken.

This decision was made by the Director General Lena Lindgren Schelin after

presentation by lawyer Elin Hallström. At the final processing has

also General Counsel Hans-Olof Lindblom, Unit Manager Malin Blixt and

unit manager Katarina Tullstedt participated. The IT security specialist Johan

Ma has participated in the assessments concerning information security.

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

Appendix

How to pay penalty fee

Copy for information to:

Data protection officer for the State Service Center

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

on 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.