Decision

Diary no

2020-12-17

DI-2019-7057

Your diary no

A325.192/2019

The police authority

Box 12256

102 26 Stockholm

Supervision according to the Criminal Data Act (2018:1177) –

The police authority's procedures for handling

personal data incidents

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

The Swedish Data Protection Authority's decision

The Swedish Data Protection Authority announces the following recommendations with the support of ch. 5. Section 6 of the Criminal Data Act (2018:1177):

1. The police authority should regularly evaluate the effectiveness of the security measures taken to detect personal data incidents and, if necessary, revise these in order to maintain adequate protection of personal data.

2. The police authority should regularly check that the routines for handling of personal data incidents is followed.

3. The police authority should, in the authority's procedures for documentation of personal data incidents, supplement with the effects that follow with an incident and what corrective actions have been taken reason for it. In addition, the Police Authority should regularly check that the procedures for documentation of personal data incidents are followed.

4. The police authority should provide its employees with ongoing information and recurrent training in the handling of personal data incidents

and about the reporting obligation.

The Swedish Data Protection Authority closes the case.

Account of the supervisory matter

The obligation of the personal data controller – i.e. private and public actors - to report certain personal data incidents to the Swedish Data Protection Authority was introduced on 25 May 2018 through the Data Protection Regulation1 (GDPR). The corresponding notification obligation was introduced on 1 August 2018 in the crime data act (BDL) for so-called competent authorities.2 The obligation to reporting personal data incidents (hereinafter referred to as incident) aims to strengthen privacy protection by the Data Inspectorate receiving information about the incident and may choose to take action when the inspection judges that it is needed for the personal data controller to handle the incident in one go satisfactory way and take measures to prevent something like that occurs again.

A personal data incident is according to ch. 1 § 6 BDL a security incident which leads to accidental or unlawful destruction, loss or alteration, or unauthorized disclosure of or unauthorized access to personal data. IN the preparatory work for the law states that it is usually an unplanned one event that affects the security of personal data in a negative way and which entail serious consequences for the protection of the data.3 One personal data incident can be, for example, that personal data has been sent to the wrong recipient, that access to the personal data has been lost, that computer equipment that stores personal data has been lost or stolen, that

someone inside or outside the organization accesses information like that

lacks authorization to.

A personal data incident that is not quickly and appropriately addressed can

entail risks for the data subject's rights or freedoms. An incident can

lead to physical, material or immaterial damage through, for example

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on that

free flow of such data and on the repeal of Directive 95/46/EC (general

data protection regulation).

2 A competent authority is according to ch. 1 § 6 BDL an authority that processes

personal data for the purpose of preventing, preventing or detecting criminal activity, investigate

or prosecuting offences, enforcing criminal penalties or maintaining public order and

security.

3 Prop.2017/18:232 p. 438

discrimination, identity theft, identity fraud, damaged reputation,

financial loss and breach of confidentiality or confidentiality.

There can be many reasons why a personal data incident occurs. Of

Datainspektionen's report series Reported personal data incidents under

period May 2018 - December 2019 it appears that the most common causes

behind the reported incidents was i.a. the human factor, technical errors,

antagonistic attacks as well as deficiencies in organizational routines or processes.4

The Data Inspectorate has initiated this supervisory case against the Swedish Police Agency i

purpose of checking whether the authority has routines in place to detect
personal data incidents and whether the authority has and has had routines for
to handle personal data incidents according to the Criminal Data Act. In the review
also includes checking whether the Swedish Police Agency has routines for
documentation of incidents that meet the requirements of
the crime data regulation (BDF) and whether the authority has implemented
information and training efforts regarding personal data incidents.
The inspection began with a letter to the Police Authority on 19 June 2019
and was followed up with a request for completion on 28 January 2020 as well as
on 12 May 2020. The authority's response to the supervisory letter was received on 19
September 2019 and the additions were received on March 6, 2020 respectively
on May 28, 2020.

Applicable regulations

The person in charge of personal data must according to ch. 3. § 2 BDL, by appropriate means
technical and organizational measures, ensure and be able to demonstrate that
the processing of personal data is constitutional and that it
data subject's rights are protected. This means that competent authorities,
by means of these measures, shall not only ensure that
the data protection regulations are followed but must also be able to demonstrate that this is the case. Which

See the Swedish Data Protection Authority's report series on Reported personal data incidents 2018
(Datainspektionen's report 2019:1) p 7 f; Reported personal data incidents January September 2019 (Data inspection report
2019:3) p.10 f. and Reported
personal data incidents 2019 (Datainspektionen's report 2020:2) p. 12 f.

technical and organizational measures required to protect

personal data is regulated in ch. 3. § 8 BDL.

In the preparatory work for the law, it is stated that organizational measures referred to in § 2 are

i.a. to have internal strategies for data protection, to inform and educate

the staff and to ensure a clear division of responsibilities. Measures such as

taken to show that the processing is constitutional can e.g. be

documentation of IT systems, treatments and measures taken and

technical traceability through logging and log follow-up. What actions that

must be taken may be decided after an assessment in each individual case.5 The measures must

reviewed and updated as necessary. The actions that it

personal data controller must take according to this provision must according to ch. 3

§ 1 BDF be reasonable taking into account the nature, scope,

context and purpose and the particular risks of the treatment.

Of ch. 3 § 8 BDL states that the person in charge of personal data must take

appropriate technical and organizational measures to protect them

personal data that is processed, especially against unauthorized or unauthorized persons

processing and against loss, destruction or other accidental damage. IN

the preparatory work for the Crime Data Act states that the security must include

equipment access protection, data media control, storage control,

user control, access control, communication control, input control,

transport control, recovery, operational security and data integrity. This one

However, the enumeration is not exhaustive. As an example of organizational

security measures may include the establishment of a security policy,

checks and follow-up of security, training in data security and

information about the importance of following current safety procedures. Routines for

notification and follow-up of personal data incidents also constitute such

actions.6

What circumstances should be considered to achieve an appropriate level of protection

is regulated in ch. 3. § 11 BDF. The measures must achieve a level of security

which is appropriate taking into account the technical possibilities, the costs of

the measures, the nature, extent, context and purpose of the processing, as well as

the particular risks of the treatment. Special consideration should be given in which

5

6

Prop. 2017/18:232 p. 453

Prop. 2017/18:232 p. 457

extent to which sensitive personal data is processed and how privacy-sensitive

other personal data processed are.7 Violation of regulations i

3 chap. §§ 2 and 8 BDL can lead to penalty fees according to ch. 6. 1 § 2 BDL.

The person in charge of personal data must according to ch. 3. § 14 BDF document all

personal data incidents. The documentation must report the circumstances

about the incident, its effects and the measures taken as a result

of that. The personal data controller must document all incidents

incidents regardless of whether it must be reported to the Data Protection Authority or not.8

The documentation must enable the supervisory authority to

check compliance with the current provision. Failure to

documenting personal data incidents may result in penalty fees

according to ch. 6 § 1 BDL.

A personal data incident must also, according to ch. 3 § 9 BDL, reported to

Datainspektionen no later than 72 hours after the personal data controller

became aware of the incident. A report does not need to be made if it is

unlikely that the incident has caused or will cause any risk

for improper intrusion into the data subject's personal privacy. Of ch. 3 Section 10

BDL states that the person in charge of personal data must inform it in certain cases

data subjects affected by the incident. Failure to report a

personal data incident to the Swedish Data Protection Authority can lead to administrative

penalty fees according to ch. 6 § 1 BDL.9

Justification of the decision

The Swedish Data Protection Authority's review

In this supervisory matter, the Swedish Data Protection Authority has to take a position on

The police authority has documented procedures for detection

personal data incidents according to the Criminal Data Act and if the authority has

and has had routines for handling incidents since the BDL came into force.

The review also covers the issue of compliance with the requirement for

documentation of incidents in ch. 3 § 14 BDF. In addition, shall

The Swedish Data Protection Authority will take a decision on whether the Police Authority has carried out

Prop. 2017/18:232 p. 189 f.

Prop. 2017/18:232 p. 198

9 Liability for violations is strict. Thus, neither intent nor negligence is required to

sanction fee must be leviable, see prop. 2017/18:232 p. 481.

information and training efforts for its employees with a focus on

handling of personal data incidents according to BDL.

The review does not cover the content of the routines or training efforts

but is focused on checking that the reviewing authority has

routines in place and that it has carried out training efforts for

the employees regarding personal data incidents. The review includes

however, if the authority's procedures contain instructions to document them

information required under the Criminal Data Ordinance.

Procedures for detecting personal data incidents

The personal data that competent authorities handle within the framework of their

law enforcement and criminal investigation activities are largely off

sensitive and privacy-sensitive nature. The nature of the business sets high standards

demands on the law enforcement authorities' ability to protect them

information was recorded through the necessary protective measures in order to, among other things,

prevent an incident from occurring.

The obligation to report personal data incidents according to ch. 3 § 9 BDL

shall be interpreted in the light of the general requirements to take appropriate technical and

organizational measures, to ensure appropriate security for

personal data, which is prescribed in ch. 3 Sections 2 and 8. An ability to quickly

detecting and reporting an incident is a key factor. Because they

the law enforcement authorities must be able to live up to

the reporting requirement, they must have internal procedures and technical capabilities for

to detect an incident.

Based on the needs of the business and with the support of risk and vulnerability analyses

competent authorities can identify the areas where there is a greater risk

that an incident may occur. Based on the analyses, the authorities can then use various instruments to detect a security threat. These can be both technical and organizational measures. The starting point is that they the security measures taken must provide sufficient protection and that incidents do not shall occur.

Examples of technical measures include intrusion detectors that automatically analyzes and detects data breaches and use of log analysis tools to be able to detect unauthorized access (log deviations). An increased insight into the business's "normal" network

traffic patterns help identify things that deviate from the normal the traffic picture against, for example, servers, applications or data files.

Organizational measures can, for example, be the adoption of internal strategies for data protection relating to internal rules, guidelines, routines and various types of steering documents and policy documents.10 Guidelines and rules for handling of personal data, routines for incident management and log follow-up11 constitute examples of such strategies. Periodic follow-up of assigned permissions are another example of organizational action. In a competent authority, there must be procedures for allocation, change, removal and regular control of authorizations.12 Information to and training of staff about the incident management rules and procedures to be followed are also examples of such measures.

The Swedish Data Protection Authority's assessment

The police authority has essentially stated the following. The authority's IT environment

security is monitored continuously, around the clock, for the purpose of prevention, detection and prevent, for example, IT attacks, operational disruptions and the spread of malware code. As a result, more serious personal data incidents can be detected in one go early stage. If there is reason for further investigation of user activities, log extracts can be used. In addition to this, each individual has employees have their own responsibility to report all incidents where there is a risk that information has been damaged, altered, destroyed, deleted or someone may have been given unauthorized access to information. Regarding organizational measures it appears from the investigation that the Police Agency has routines for reporting personal data incidents internally and that it is available on the authority's intranet information on how and when reporting must be done. The police authority has also developed a general information security training, as under spring 2019 made available to all employees at the authority. IN the training includes a section on incidents, which also includes personal data incidents. The authority now makes a requirement that all employees must complete the training to gain access to the authority's IT system.

Crime Data Act - Partial report of the Inquiry into the 2016 data protection directive Stockholm 2017, SOU 2017:29 p. 302

11 Competent authorities must ensure that there are routines for log follow-up, see prop. 2017/18:232 p. 455 f.

12 3 ch. § 6 BDL and supplementary provisions in ch. 3. § 6 BDF

The Data Inspectorate can state that the Police Agency has routines to

detect personal data incidents on the spot.

The duty to take security measures to detect

personal data incidents are not tied to a specific time but the actions

must be continuously reviewed and, if necessary, changed. For the Police Authority

must be able to maintain a sufficient level of protection of personal data over time

recommends the Data Inspectorate, with the support of ch. 5. § 6 BDL, that

the authority regularly evaluates the effectiveness of those taken

the security measures to detect personal data incidents and that

the authority updates these if necessary.

Procedures for handling personal data incidents

In order to live up to the requirements for organizational measures in ch. 3. Section 8

BDL, the personal data controller must have documented internal routines that

describes the process to be followed when an incident has been detected or

occurred, including how the incident will be contained, managed and recovered,

as well as how the risk assessment should be carried out and how the incident should be reported internally

and to the Swedish Data Protection Authority. The routines must include, among other things, what a

personal data incident is/can be, when an incident needs to be reported, and

to whom, what must be documented, the distribution of responsibilities and which

information that should be provided within the framework of notification to

The Swedish Data Protection Authority.

The Swedish Data Protection Authority's control of procedures for handling

personal data incidents refer to the time from the entry into force of the Criminal Data Act

i.e. on August 1, 2018.

The Swedish Data Protection Authority's assessment

The police authority has essentially stated the following. Of information on

The police agency's intranet shows how a report of a

personal data incident must be handled. Personal data incidents are handled as

other types of incidents and are reported in the authority's

incident management system POINT. In a supplementary answer clarify

The police authority that it is true that there were no national ones

guidelines for handling personal data incidents when the BDL entered into force

but this does not mean that routines were lacking. The routines have been developed by

the legal department and the data protection officer in consultation with the IT department, they

have been documented within the legal department and have thus been available

for the people who work with managing and assessing

personal data incidents. Information about what can be a

personal data incident and what an employee should do about him or her

suspect that such an event has occurred, among other things, has been found on the police intranet

and in basic data protection training.

It also appears that the authority before the introduction of the Criminal Data Act did

an assessment that existing structures and systems for incident reporting

could also be used to detect, report and manage

personal data incidents. At that time the Police Authority considered that they

routine documents that existed were sufficient even to manage

personal data incidents. With this in mind, it was initially prepared

no new national guidelines, only an internal one was made

division of responsibilities and unit-specific routines for handling measures.

However, the police authority has drawn attention to an increased need to in guidelines

formalize the routines that were previously developed. This is to clarify
the distribution of responsibilities and roles between different organizational units and create
a greater awareness of the importance of identifying and reporting
personal data incidents throughout the authority. The police authority states
furthermore, that the authority has continuously evaluated and updated its
written procedures on how personal data incidents are to be handled since the new ones
the data protection rules began to be applied in the summer of 2018. Routines to
handling personal data incidents has thus existed since the summer of 2018.
The latest version Personal data incident procedure dated 2020-05-28 has
submitted by the authority. The police authority has also submitted it
information from the authority's intranet that has been available to everyone
employee since July 2018.
Taking into account the submitted documents and what appeared in
case, the Swedish Data Protection Authority states that the Police Authority from the time
when the Criminal Data Act came into force had and still have routines to deal with
personal data incidents on site.
To be able to handle detected personal data incidents correctly
and counteract its effects and risks for the data subjects' personal lives
integrity is important. The Swedish Data Protection Authority therefore recommends, with the support of
5 ch. § 6 BDL, that the Police Authority regularly checks that the routines
for handling personal data incidents is followed.

Procedures for documentation of personal data incidents
A prerequisite for the Data Inspection Authority to be able to check

compliance with the documentation requirement of incidents in ch. 3. § 14 BDF is that
the documentation includes certain information that should always be included.
The documentation must include all details of the incident, including its
reasons, what happened and the personal data affected. It should also
contain the consequences of the incident and the corrective actions that it takes
taken by the data controller.

The Swedish Data Protection Authority's assessment

The police authority has mainly stated the following. The authority
uses the incident management system POINT for reporting e.g.
personal data incidents. The legal department documents the events that
is deemed to be a personal data incident in a special order. Of
the legal department's documentation contains information about, among other things date then
the incident was discovered, the date the incident was judged to be a
personal data incident, a brief description of the personal data incident,
current legislation (the Data Protection Ordinance or the Criminal Data Act). Further
also appears if the incident has been reported to the Data Inspectorate,
case number in POINT and any case number in the Police's general
diarium (PÄR) which is used if the case has been reported to the Data Inspectorate as well as
a legal assessment with possible basis and possible views
from the data protection officer.

The Swedish Data Protection Authority states that the Police Authority has an internal IT system
in order to e.g. report personal data incidents. In addition, it appears from
the legal department's documentation to some extent which information should
be documented. The Swedish Data Protection Authority notes, however, that from the description
it is not clear which effects accompany an incident and which corrective ones
measures taken in connection with it.

Being able to document personal data incidents that have occurred in an accurate manner way and thus counteract the risk of the documentation being deficient or incomplete is important. Insufficient documentation can lead to the incidents are not handled and remedied correctly, which can get impact on privacy protection. The Swedish Data Protection Authority therefore recommends, with the support of ch. 5 § 6 BDL, that the Police Authority's routines for documentation of personal data incidents is supplemented with the data as stated in the paragraph above. In addition, the Police Authority should implement

regular checks of the internal documentation of personal data incidents.

Information and training regarding personal data incidents

The staff is an important resource in security work. It's just not enough internal procedures, rules or governing documents if users do not follow them. All users must understand that handling of personal data must take place in one legally secure way and that it is more serious not to report an incident yet to report e.g. a mistake or an error. It is therefore required that all users receive adequate training and clear information about data protection. The person in charge of personal data must inform and train his staff in matters on data protection including handling of personal data incidents. Of Datainspektionen's report series Reported personal data incidents under period 2018-2019, it appears that the human factor is the most common the cause of reported personal data incidents. 13 These mainly consist of individuals who, knowingly or unknowingly, do not follow internal procedures at

processing of personal data or committed a mistake in the handling of

personal data. About half of the incidents are due to it

the human factor is about misdirected letters and e-mails.

According to the Swedish Data Protection Authority, this underlines the importance of

internal procedures and technical security measures need to be supplemented with

ongoing training, information and other measures to increase knowledge and

awareness among employees.

The Swedish Data Protection Authority's assessment

When asked how information and training about incidents is provided

employees, the Police Authority has stated i.a. following. At the authority's

intranet there is information on reporting personal data incidents. All

new employees in the IT department undergo a

training on information security incidents and incident management.

The authority has also produced general training in

information security that was made available to everyone in the spring of 2019

coworker. The police authority now requires that all employees

Report 2019:1, report 2019:3 and report 2020:2. Similar conclusions have been drawn by MSB

its annual report for serious IT incidents, i.e. that most of the incidents are due to

human mistakes, see https://www.msb.se/sv/aktuellt/nyheter/2020/april/arsrapporten-forallvarliga-it-incidenter-2019-ar-slappt/

13

must complete the training to gain access to the authority's IT system. IN

the training includes a section on incidents, which also includes

personal data incidents. The section contains, among other things, examples of which

incidents to be reported in POINT. In addition to this training, there is a
several data protection training courses in the authority's learning platform, where i.a.
personal data incidents are described and the importance of reporting these is emphasized.
The police authority has submitted the authority's manual regarding
"Basic data protection training" and "Training in the EU's
data protection regulation". The manuals show a section on handling of
personal data incidents. The basic data protection training aims
itself to all employees within the Police Authority with access to the police
computer system. The training is also aimed at consultants and others
contractors who process information automatically within the framework of
his mission. The training in the EU's data protection regulation is primarily aimed at
those who, in their work, process personal data in different ways within the police
non-law enforcement activities. A corresponding education is available for
personal data processing within the scope of the Criminal Data Act.
Against the background of what appears from the investigation, the Data Protection Authority believes
that the Police Authority has shown that the authority has provided information and
training on handling personal data incidents to its employees.
To maintain competence and ensure that new staff get
training, it is important to have recurring information and training
the employees and hired personnel. The Swedish Data Protection Authority recommends, with
support of ch. 5 § 6 BDL, that the Police Authority provides the employees on an ongoing basis
information and recurring training in the handling of
personal data incidents and the obligation to report them.
This decision has been made by unit manager Charlotte Waller Dahlberg after
presentation by lawyer Maria Angelica Westerberg. At the final
IT security specialist Ulrika is also handling the case

Sundling and the lawyer Jonas Agnvall participated.

Charlotte Waller Dahlberg, 2020-12-17 (This is an electronic signature)

Copy for the attention of:

The police authority's data protection officer

How to appeal

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

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

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.