

Decision

Diariennr

2020-12-17

DI-2019-7057

Ert diariennr

A325.192 / 2019

The police authority

Box 12256

102 26 Stockholm

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

The police authority's routines for handling

personal data incidents

Table of Contents

The Data Inspectorate's decision	2
Report on the supervisory matter	3
Applicable provisions	4
Grounds for the decision	6
The Data Inspectorate's review	6
Procedures for detecting personal data incidents	7
The Data Inspectorate's assessment	8
Routines for handling personal data incidents	9
The Data Inspectorate's assessment	9
Procedures for documentation of personal data incidents	10
The Data Inspectorate's assessment	11
Information and training on personal data incidents	12
The Data Inspectorate's assessment	12

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

1 (14)

The Data Inspectorate

DI-2019-7057

The Data Inspectorate's decision

The Data Inspectorate announces the following recommendations with the support of ch.

Section 6 of the Criminal Data Act (2018: 1177):

1.

The police authority should regularly evaluate their effectiveness

precautions taken to detect

personal data incidents and, if necessary, revise them 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 routines for documentation of

personal data incidents, supplement with the effects that follow

with an incident and what corrective measures have been taken

occasion of 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

recurring training in the handling of personal data incidents

and on the reporting obligation.

The Data Inspectorate closes the case.

2 (14)

The Data Inspectorate

DI-2019-7057

Report on the supervisory matter

The obligation for the personal data controller - ie. private and public

actors - to report certain personal data incidents to the Data Inspectorate

was introduced on 25 May 2018 by the Data Protection Regulation¹ (GDPR).

A corresponding notification obligation was introduced on 1 August 2018 in

the Criminal Data Act (BDL) for so-called competent authorities.² The obligation to

report personal data incidents (hereinafter referred to as incidents) aims to strengthen

privacy protection by the Data Inspectorate receiving information about

the incident and may choose to take action when the inspectorate deems it appropriate

is needed for the personal data controller to handle the incident on one

satisfactorily and take steps to prevent something similar

occurs again.

According to ch. 1, a personal data incident is § 6 BDL a security incident that

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 a question of an unplanned

event that adversely affects the security of personal data

and which have serious consequences for the protection of data.³ En

personal data incident may, for example, be 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 takes part in information like that lacks authority to.

A personal data incident that is not dealt with quickly and appropriately can entail risks to the data subject's rights or freedoms. An incident can lead to physical, material or intangible damage by, for example

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on that free flow of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).

2 A competent authority is in accordance with ch. § 6 BDL an authority that deals personal data for the purpose of preventing, deterring or detecting criminal activities, investigating or prosecute crimes, enforce criminal sanctions or maintain public order and security.

3 Prop.2017 / 18: 232 pp. 438

1

3 (14)

The Data Inspectorate

DI-2019-7057

discrimination, identity theft, identity fraud, damaged reputation, financial loss and breach of confidentiality or secrecy.

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

The Swedish Data Inspectorate's report series Reported personal data incidents under

The period May 2018 - December 2019 shows that the most common causes

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

antagonistic attacks and shortcomings in organizational routines or processes.⁴

The Data Inspectorate has initiated this supervisory case against the Police Authority in

purpose to check whether the authority has procedures 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 Police Authority has routines for documentation of incidents that meet the requirements of the Criminal Data Ordinance (BDF) and whether the authority has implemented information and training initiatives on 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 on 12 May 2020. The authority's response to the supervisory letter was received on 19 September 2019 and the supplements were received on March 6, 2020 respectively on May 28, 2020.

Applicable regulations

According to ch. 3, the person responsible for personal data must § 2 BDL, by appropriate technical and organizational measures, ensure and be able to demonstrate that the processing of personal data is in accordance with the constitution and that it data subjects' rights are protected. This means that competent authorities,

Using these measures, should not just ensure that the data protection regulations are followed but must also be able to show that this is the case. Which

See the Data Inspectorate's report series on Reported Personal Data Incidents 2018

(Datainspektionens rapport 2019: 1) p 7 f; Reported personal data incidents January-September 2019 (Datainspektionen's 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. 8 § BDL.

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

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

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

taken to show that the treatment is in accordance with the constitution, e.g. be

documentation of IT systems, treatments and measures taken and

technical traceability through logging and log monitoring. What measures

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

reviewed and updated as needed. The measures it

the person responsible for personal data shall take in accordance with this provision shall, in accordance with ch.

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

context and purpose and the specific risks of the treatment.

Of ch. 3 Section 8 of the BDL states that the person responsible for personal data shall take

appropriate technical and organizational measures to protect them

personal data processed, in particular against unauthorized or unauthorized use

treatment and against loss, destruction or other unintentional damage. IN

The preparatory work for the Criminal Data Act states that security must include

access protection for equipment, control of data media, storage control,

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

transport control, restoration, reliability and data integrity. This

enumeration, however, is not exhaustive. As an example of organizational

security measures include the establishment of a security policy,

security controls and follow-up, computer security training and

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

reporting and follow-up of personal data incidents also constitute such measures.⁶

What circumstances should be taken into account in order to achieve an appropriate level of protection is regulated in ch. 11 § BDF. The measures must achieve a level of safety appropriate taking into account the technical possibilities, the costs of the measures, the nature, scope, context and purpose of the treatment, and the specific risks of the treatment. Special consideration should be given in which

5

6

Prop. 2017/18: 232 pp. 453

Prop. 2017/18: 232 pp. 457

5 (14)

The Data Inspectorate

DI-2019-7057

the extent to which sensitive personal data is processed and how sensitive to privacy other personal data processed is.⁷ Violation of provisions in

Chapter 3 2 and 8 §§ BDL can lead to sanction fees according to ch. 1 § 2 BDL.

According to ch. 3, the person responsible for personal data must § 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 person responsible for personal data must document all that occurred

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

The documentation must enable the supervisory authority to:

check compliance with the provision in question. Failure to

documenting personal data incidents can lead to penalty fees

according to ch. 6 1 § BDL.

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

The Data Inspectorate no later than 72 hours after the person responsible for personal data

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

it is unlikely that the incident has or will entail any risk

for undue invasion of the data subject's privacy. Of ch. 3 § 10

BDL states that the person responsible for personal data must in certain cases inform it

registered affected by the incident. Failure to report one

personal data incident to the Data Inspectorate can lead to administrative

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

Justification of the decision

The Data Inspectorate's review

In this supervisory matter, the Data Inspectorate has a position to decide on

The police authority has documented routines for detecting

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

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

The Data Inspectorate will decide whether the Police Authority has implemented

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

Prop. 2017/18: 232 pp. 198

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

it must be possible to charge a penalty fee, see bill. 2017/18: 232 pp. 481.

7

8

6 (14)

The Data Inspectorate

information and training initiatives for its employees with a focus on handling of personal data incidents according to BDL.

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

but is focused on verifying that the reviewing authority has

routines on site and that it has implemented training initiatives for

employees regarding personal data incidents. The review includes

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

information required by the Criminal Data Regulation.

Routines for detecting personal data incidents

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

law enforcement and crime investigation activities are to a large extent of

sensitive and privacy sensitive nature. The nature of the business is high

requirements on the ability of law enforcement agencies to protect them

information was registered through the necessary protection measures to e.g.

prevent an incident from occurring.

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

shall be construed 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. 2 and 8 §§. An ability to fast

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

law enforcement agencies must be able to live up to

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

to detect an incident.

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

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

that an incident may occur. Based on the analyzes, 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 safety measures taken must provide adequate protection and that incidents do not should occur.

Examples of technical measures include intrusion detectors as automatic analyzes and detects data breaches and the use of log analysis tool to detect unauthorized access (log deviations). An increased insight into the business' "normal" network

7 (14)

The Data Inspectorate

DI-2019-7057

traffic patterns help to identify things that deviate from the normal

the traffic picture towards, 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 different types of governing documents and policy documents.¹⁰ Guidelines and rules for handling personal data, routines for incident management and log follow-up¹¹ constitute examples of such strategies. Periodic follow-up of assigned authorizations is another example of organizational measures. In a competent authority, there shall be procedures for allocation, change, removal and regular verification of privileges.¹² Information and training of staff on the rules and routines for incident management to be followed also examples of such measures.

The Data Inspectorate's assessment

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

security monitored continuously, around the clock, in order to prevent, detect and prevent, for example, cyber-attacks, malfunctions and the spread of malware code. Thereby, more serious personal data incidents can be detected in one 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 a personal responsibility to report all incidents where there is a risk information has been damaged, altered, destroyed, cleared or someone may have been given unauthorized access to information. Regarding organizational measures

The investigation shows that the Police Authority has routines for reporting personal data incidents internally and that it is on the authority's intranet information on how and when the reporting is to be done. The police authority has in addition, 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 requires that all employees must complete the training to gain access to the authority's IT system.

Criminal Data Act - Partial report by the Inquiry into the 2016 Data Protection Directive Stockholm 2017, SOU 2017: 29 pp. 302

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

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

10

8 (14)

The Data Inspectorate

DI-2019-7057

The Data Inspectorate can state that the Police Authority has routines for detect personal data incidents on site.

The obligation to take precautionary measures to detect personal data incidents are not linked to a specific time but the measures shall be continuously reviewed and, if necessary, changed. To the Police Authority must be able to maintain an adequate level of protection of personal data over time recommends the Data Inspectorate, with the support of ch. § 6 BDL, att the authority regularly evaluates the effectiveness of those taken security measures to detect personal data incidents and that the authority updates these if necessary.

Routines for handling personal data incidents

In order to be able to live up to the requirements for organizational measures in ch. § 8 BDL, the person responsible for personal data must have documented internal routines such as describes the process to be followed when an incident has been detected or occurred, including how to limit, manage and recover the incident, and how the risk assessment is to be carried out and how the incident is to be reported internally and to the Data Inspectorate. The routines must state e.g. what a personal data incident is / can be, when an incident needs to be reported, and to whom, what is to be documented, the division of responsibilities and which information that should be provided in the context of notification to The Data Inspectorate.

The Data Inspectorate's control of routines 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 Data Inspectorate's assessment

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

The police authority's intranet shows how a reporting of a personal data incident must be handled. Personal data incidents are handled as other types of incidents and are reported in the authority incident management system POINT. In a supplementary answer clarifies The police authority that it is true that there were no national guidelines for handling personal data incidents when BDL came 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, de has been documented within the legal department and has thus been available

9 (14)

The Data Inspectorate

DI-2019-7057

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 suspects that such an incident has occurred, among other things, on the police's intranet and in basic data protection training.

It also appears that the authority before the introduction of the Criminal Data Act did an assessment of 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 were available were also sufficient to handle personal data incidents. Due to this, it was initially prepared no new national guidelines but only an internal one division of responsibilities and unit-specific routines for measures in handling.

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

formalize the routines previously developed. This is to clarify the division 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 further that the authority has continuously evaluated and updated its written routines on how personal data incidents should be handled since the new ones the data protection rules began to be applied in the summer of 2018. Routines for that dealing with personal data incidents has thus existed since the summer of 2018.

Latest version Routine for personal data incident 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 accessible to all employees since July 2018.

Taking into account the documents submitted and what has emerged in the case, the Data Inspectorate states that the Police Authority from the time when the Criminal Data Act came into force has had and has routines for dealing with personal data incidents on site.

To be able to handle discovered personal data incidents in a correct way and counteract its effects and risks on the data subjects' personalities Integrity is important. The Data Inspectorate therefore recommends, with the support of Chapter 5 § 6 BDL, that the Police Authority regularly checks that the routines for handling personal data incidents is followed.

10 (14)

The Data Inspectorate

DI-2019-7057

Routines for documentation of personal data incidents

A prerequisite for the Data Inspectorate to be able to check

compliance with the documentation requirement of incidents in ch. § 14 BDF is that

the documentation includes certain information that should always be included.

The documentation shall include all details of the incident, including its

reasons, what happened and the personal data involved. It should too

contain the consequences of the incident and the corrective actions taken

personal data controller has taken.

The Data Inspectorate's assessment

The police authority has mainly stated the following. The authority

uses the incident management system POINT for reporting of e.g.

personal data incidents. The Legal Department documents the events that

is considered to be a personal data incident in a special order. Of

the legal department's documentation provides information on e.g. date then

the incident was discovered, the date when the incident was judged to be one

personal data incident, a brief description of the personal data incident,

current legislation (the Data Protection Ordinance or the Criminal Data Act). Further

appears even if the incident has been reported to the Data Inspectorate,

case number in POINT and possibly case number in the Police General

diarium (PÄR) which is used if the matter is reported to the Data Inspectorate and

a legal assessment with any basis and any comments

from the Data Protection Officer.

The Data Inspectorate states that the Police Authority has an internal IT system

to e.g. report personal data incidents. In addition, it appears from

the legal department's documentation to some extent what information is to be provided

documented. However, the Data Inspectorate notes that from the description

it is not clear what effects come with an incident and what corrective measures

measures taken in response to it.

To be able to document occurred personal data incidents correctly and thereby counteract the risk of the documentation becoming deficient or incomplete is important. Inadequate documentation can lead to the incidents are not handled and remedied properly, which can get impact on privacy protection. The Data Inspectorate 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 specified in the paragraph above. In addition, the Police Authority should implement

1 1 (14)

The Data Inspectorate

DI-2019-7057

regular inspections of the internal documentation of personal data incidents.

Information and education about personal data incidents

The staff is an important resource in the security work. It's not just enough internal procedures, rules or governing documents if users do not follow them.

All users must understand that the handling of personal data must take place in one go legally secure and that it is more serious not to report an incident than to report e.g. a mistake or a mistake. It is therefore required that everyone users receive adequate training and clear information on data protection.

The person responsible for personal data must inform and train his staff in matters on data protection including the handling of personal data incidents. Of

The Swedish Data Inspectorate's report series Reported Personal Data Incidents under in the 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, consciously or unconsciously, do not follow internal routines

processing of personal data or made a mistake in handling

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

The human factor is about misplaced letters and emails.

In the Data Inspectorate's opinion, this underlines the importance of

internal routines and technical safety measures need to be supplemented with

ongoing training, information and other measures to increase knowledge and

awareness among employees.

The Data Inspectorate's assessment

On the question of how information and education about incidents is provided

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

intranet contains information on reporting personal data incidents. All

new employees in the IT department undergo one during their introduction

training on information security incident and incident management.

The authority has also developed a general education in

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

coworker. The police authority now demands that all employees

Report 2019: 1, report 2019: 3 and report 2020: 2. MSB has drawn similar conclusions

its annual report for serious IT incidents, ie. that most of the incidents are due

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

13

1 2 (14)

The Data Inspectorate

DI-2019-7057

shall 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 one several data protection educations in the authority's learning platform where e.g. personal data incidents are described and the importance of reporting these is pointed out.

The police authority has submitted the authority's manual regarding

"Basic data protection training" and "Training in the EU

Data Protection Regulation ". The manuals contain a section on handling

personal data incidents. The basic data protection training focuses

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

its mission. The training in the EU Data Protection Regulation is mainly aimed at

those who in their work process personal data within the police in different ways

non-law enforcement activities. A corresponding education is available for

personal data processing within the area of the Criminal Data Act.

In the light of what appears from the investigation, the Data Inspectorate considers

that the Police Authority has shown that the authority has provided information and

training on the handling of personal data incidents to their employees.

To maintain competence and ensure that new staff receive

education, recurring information and education is important

the employees and hired staff. The Data Inspectorate recommends, with

support of ch. 5 § 6 BDL, that the Police Authority provides the employees on an ongoing basis

information and recurrent training in the management of

personal data incidents and the obligation to report them.

This decision was made by unit manager Charlotte Waller Dahlberg after

presentation by lawyer Maria Angelica Westerberg. At the final

The IT security specialist Ulrika also handles the case

Sundling and the lawyer Jonas Agnvall participated.

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

1 3 (14)

The Data Inspectorate

DI-2019-7057

Copy for information to:

The police authority's data protection officer

How to appeal

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

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

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

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

The Data Inspectorate forwards it to the Administrative Court in Stockholm

examination.

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

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

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

1 4 (14)