Decision

Diarienr

2020-12-17

DI-2019-7058

Ert diarienr

EBM2019-572

The Economic Crime Authority

The unit of law

Box 22098

101 36 STOCKHOLM

Supervision of the Criminal Data Act (2018: 1177) -

The Swedish Environmental Crime Agency's routines for handling

of personal data incidents

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 announces the following recommendations with the support of ch.

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

1.

The Economic Crimes Authority should regularly evaluate the effectiveness of

the security measures taken to detect

personal data incidents and, if necessary, revise them in order to

maintain adequate protection of personal data.

2. The Economic Crime Authority should regularly check that the procedures for

handling of personal data incidents is followed.

The Economic Crime Authority should regularly check that the internal

the procedures for documentation of personal data incidents are followed.

4. The Economic Crimes 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.

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

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 Swedish Environmental Crime Agency

in order 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 Swedish Environmental Crime Agency 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 Swedish Environmental Crime Agency on 19 June 2019 and was followed up with a request for supplementation on 28 January 2020. The authority's response to the supervisory letter was received on 25 September 2019 and The supplement was received on 18 February 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 technical and organizational measures required to protect personal data is regulated in ch. 8 § BDL.

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.

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

5

6

7

Prop. 2017/18: 232 pp. 453

Prop. 2017/18: 232 pp. 457

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

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 decision

The Data Inspectorate's review

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

The Swedish Environmental Crime Agency has routines for detecting personal data incidents

according to the Criminal Data Act and if the authority has and has had routines for that

handle incidents since the BDL came into force. The review also includes

the question of compliance with the requirement for documentation of incidents in ch. 14

§ BDF. In addition, the Data Inspectorate must decide whether

The Swedish Environmental Crime Agency has implemented information and training initiatives

Prop. 2017/18: 232 pp. 198

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.

8

9

for its employees with a focus on handling 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

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 Economic Crimes Authority has mainly stated the following. The authority

processes personal data for law enforcement purposes primarily in

operating systems, software and storage space provided by

The Police Authority and the Public Prosecutor's Office. In the Economic Crimes Authority criminal investigation activities, the Police Authority's operational support is used Durtvå13 and in their prosecution activities the Public Prosecutor's Office is used operational support Cåbra.14 This means that these two authorities are personal data assistants to the Swedish Environmental Crime Agency. The Economic Crime Authority has in a personal data assistant agreement with the Public Prosecutor's Office ensured that routines for detecting incidents are in place. It has further emerged that the assistant agreement with the Police Authority regarding the IT system Durtvå vid the time for the Economic Crimes Authority's response had not yet been completed. Furthermore, the Economic Crimes Authority has stated that the Public Prosecutor's Office regularly performs logging in their systems as well as that of the Police Authority IT environment is continuously security monitored in order to prevent, detect and prevent, for example, cyber attacks, malfunctions and the spread of malware code. As a result, more serious personal data incidents can be detected. If

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

13 Computerized investigation routine with coercive measures

14 Central system for the prosecution service's criminal case management

there is reason for further investigation of user activities can

log extracts are used. Regarding the Swedish Environmental Crime Agency's own
IT infrastructure is stated to be monitored and logged regularly, e.g. in order to
it must be possible to detect personal data incidents. In addition, the authority has
a policy for handling security logs in IT systems at
The Swedish Environmental Crime Agency (EBM A-2012/0135). Regarding organizational
measures, the Swedish Environmental Crime Agency has developed routines for
authorization granted to the Public Prosecutor's Office, and authorizations are followed
up and cleaned continuously. The Economic Crimes Authority has also implemented
training and information initiatives on the new data protection regulation for
without staff. These have included information on personal data incidents and
on reporting obligations. The purpose has been to make the staff aware
thereby increasing the propensity to report incidents.

As can be seen from the investigation, the Police Authority and the Public Prosecutor's Office
personal data assistant to the Swedish Environmental Crime Agency regarding IT systems
Durtvå and Cåbra respectively. The Data Inspectorate wants to emphasize that it is incumbent upon
The Economic Crime Authority, in its capacity as personal data controller, to insure
ensure that the personal data assistants take appropriate security measures to:
protect the personal data for which the Economic Crimes Authority is responsible.

The Data Inspectorate can state that the Swedish Environmental Crime Agency has routines for
to 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. In order to
The economic crime authority must be able to maintain a sufficient level of protection of
personal data over time, the Data Inspectorate recommends, with the support of
Chapter 5 § 6 BDL, that the authority regularly evaluates the effectiveness of those

the security measures taken 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 Economic Crimes Authority has i.a. stated the following. The authority has, since

a number of years ago, documented routines for incident management. Further

The authority has stated that in the autumn of 2018 it identified a need

to clarify what applies to the handling of personal data incidents,

why work began on developing guidelines for this. The work

was completed by the authority on 18 September 2019 deciding on new ones

guidelines for handling personal data incidents - EBMR-A 2019: 3. To

the guideline also includes Routine in the event of loss of physical data media and incorrectly sent email, step by step and

Routine in the event of IT incidents involving personal data,

gradually. The Swedish Environmental Crime Agency has also submitted documentation

regarding the authority's previous routines and about incident reporting systems

(Key Concept), which shows that these also included reporting of

personal data incidents.

Taking into account the documents submitted and what has emerged in

In this case, the Data Inspectorate states that the Swedish Environmental Crime Agency from

the time when the Criminal Data Act came into force has had and has routines for

handle 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 Economic Crimes Authority regularly checks that

the procedures for handling personal data incidents are followed.

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 Economic Crimes Authority has mainly stated the following. The authority uses the Key Concept incident management system for internal reporting of i.a. personal data incidents. The authority's data protection officer is recipient of the internal reports of incidents in the system and is it which decides whether the incidents are to be reported to the Data Inspectorate. An incident which is reported to the Data Inspectorate is also recorded in the record keeping system Cårall. The Swedish Environmental Crime Agency has developed a guideline for handling personal data incidents and a questionnaire for this purpose.

The Data Inspectorate states that the Swedish Environmental Crime Agency has an IT system to e.g. report incidents involving personal data. In addition appears from the authority's new guidelines for handling personal data incidents that all incidents must be documented and which information that the documentation must include. The Data Inspectorate states that the Swedish Environmental Crime Agency's routines for documentation meet the requirements in the current provision.

The Data Inspectorate notes, however, that the authority has stated in its response that during 2018-2019, 15 incidents have been identified internally and that the documentation of these in some cases has been deficient. This can according to The Data Inspectorate's opinion indicates that there is ignorance among employees about what is to be documented. The Data Inspectorate therefore recommends, with the support of ch. 5 § 6 BDL, that the Economic Crimes Authority implements 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. 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 Swedish Environmental Crime Agency has stated, among other things. following. Information and
education has been provided in the form of e-education, information on the intranet and

information initiatives in connection with the new data protection regulation

took effect. The new guidelines for handling personal data incidents

has been implemented and information initiatives on this have been carried out.

Routines and rules for handling e-mail and for other information carriers

has been produced. In addition, the authority has revised the Guideline

The Swedish Environmental Crime Agency's information security - policy and responsibility (EBMR-A

2015-3) to clarify each employee's responsibility for reporting

shortcomings and incidents. The guideline states the responsibilities of employees and

executives have for the authority's information security. Further has

various guidance documents that have a bearing on the handling of

personal data incidents have been identified, e.g. The Economic Crime Authority

guidance for secure information management. These are published on

the authority's intranet.

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/

15

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

that the Economic Crimes Authority has shown that the authority has provided information

and training on the handling of personal data incidents to their

coworker.

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 Economic Crime 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.

Other

From the investigation in the case, it has emerged that at the time of

The Economic Crimes Authority's response was a negotiation with the Police Authority in

purpose of establishing a personal data assistant agreement regarding the IT system

Durtvå. The existence of such an assistant agreement is not covered by this

supervision and therefore the Data Inspectorate does not take any action in this regard

respect.

This decision was made by unit manager Charlotte Waller Dahlberg after

presentation by Maria Angelica Westerberg. At the final processing

of the case also has the IT security specialist Ulrika Sundling and the lawyer

Jonas Agnvall participated.

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

Copy for information to:

The Swedish Environmental Crime Agency'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.