Decision

Diary no

2020-12-17

DI-2019-7058

Your diary no

EBM2019-572

The Ecocrime Authority

The legal entity

Box 22098

101 36 STOCKHOLM

Supervision of the crime data act (2018:1177) –

The Ecocrime Authority's procedures 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

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 Ecocrime 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 Ecocrime Authority should regularly check that the routines for

handling of personal data incidents is followed.

3. The Ecocrime Authority should regularly check that the internal

the procedures for documentation of personal data incidents are followed.

4. The Ecocrime 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 Swedish Data Protection Authority has initiated this supervisory case against the Ecocrime Authority

in order to check 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 Ecocrime Authority 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 Ecocrime Authority on 19 June 2019 and was followed up with a request for completion on January 28, 2020. The authority's response to the supervisory letter was received on 25 September 2019 and the supplement was received on February 18, 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 technical and organizational measures required to protect personal data is regulated in ch. 3. § 8 BDL.

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 (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 § 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 processing.
Of 3 ch. § 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 extent to which sensitive personal data is processed and how privacy-sensitive other personal data processed are.7 Violation of regulations i

5

6

7

Prop. 2017/18:232 p. 453

Prop. 2017/18:232 p. 457

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

3 ch. §§ 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 integrity. 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 decisions

The Swedish Data Protection Authority's review

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

The Ecocrime Authority has routines for detecting personal data incidents

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

handling incidents since the BDL came into force. The review also covers

the question of compliance with the requirement for documentation of incidents in ch. 3. 14

§ BDF. In addition, the Swedish Data Protection Authority must take a decision on

The Ecocrime Authority has carried out information and training efforts

Prop. 2017/18:232 p. 198

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.

8

9

for its employees with a focus on handling 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 Ecocrime Authority has essentially stated the following. The authority

processes personal data for law enforcement purposes primarily i

operating systems, software and storage areas provided by

The Police Authority and the Public Prosecutor's Office. In the Ecocrime Authority
criminal investigation activities, the Police Agency's operational support is used
Durtvå13 and in their prosecutorial activities, the Prosecutor's Office's is used
operational support Cåbra.14 This means that these two authorities are
personal data assistants to the Ecocrime Authority. The Ecocrime Authority
has ensured in the personal data processing agreement with the Public Prosecutor's Office that
procedures for detecting incidents are in place. It has further emerged
that the assistance agreement with the Police Authority regarding the IT system Durtvå at
the timing of the Ecocrime Authority's response had not yet been finalized.
Furthermore, the Ecocrime Authority has stated that the Prosecutor's Office
regularly performs logging in its systems as well as that of the Police Authority
The IT environment is continuously monitored for security in order to prevent, detect and
prevent, for example, IT attacks, operational disruptions and the spread of malware
code. In this way, more serious personal data incidents can be detected. If
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
13 Computerized investigation routine with coercive means management
14 Central system for the prosecution's criminal case management

there is reason for closer investigation of user activities can

log extracts are used. Regarding the Ecocrime Authority's own
IT infrastructure is stated to be monitored and logged regularly, e.g. in order to
personal data incidents must be detectable. In addition, the authority has
a policy for handling security logs in IT systems at
The Ecocrime Authority (EBM A-2012/0135). Regarding organizational
measures, the Ecocrime Authority has developed routines for
authority allocation regarding the Public Prosecutor's Office, and authorities are followed
up and cleaned continuously. The Ecocrime Authority has also carried out
training and information efforts on the new data protection regulation for
its staff. These have included information about personal data incidents and
on reporting obligations. The purpose has been to raise awareness among the staff
and thereby increase the propensity to report incidents.

As can be seen from the investigation, the Police Authority and the Prosecutor's Office are
personal data assistant to the Eco-crimes Agency regarding the IT systems
Durtvå and Cåbra respectively. The Swedish Data Protection Authority would like to emphasize that it is incumbent
The Ecocrime Authority, in its capacity as data controller, to insure
ensure that the personal data assistants take appropriate security measures to
protect the personal data for which the Ecocrime Authority is responsible.

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

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. In order to
The Ecocrime Authority must be able to maintain a sufficient level of protection of
personal data over time recommends the Data Inspectorate, with the support of
5 ch. § 6 BDL, that the authority regularly evaluates the effectiveness of the

the security measures taken 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 Ecocrime Authority has, among other things, stated the following. The authority has, since

a number of years back, documented procedures for incident management. Further

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

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

which is why work on developing guidelines for this was started. The work

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

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

the guideline also includes the Procedure for loss of physical data media and incorrectly sent e-mail, step by step, and the

Procedure for IT incidents involving personal data,

gradually. The Ecocrime Authority has also submitted documentation

regarding the authority's previous procedures and about the incident reporting system

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

personal data incidents.

Taking into account the submitted documents and what appeared in

the case, the Data Inspectorate states that the Ecocrime Authority from

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

handle 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 Ecocrime Authority regularly checks that

the routines for handling personal data incidents are 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 Ecocrime 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 notifications of incidents in the system and is the
which determines whether the incidents must be reported to the Data Inspectorate. An incident
which is reported to the Data Inspection Authority is also entered in the diary keeping system
Carall. The Ecocrime Authority has drawn up a guideline for the handling of
personal data incidents as well as a questionnaire for this purpose.

The Swedish Data Protection Authority notes that the Ecocrime Authority has an IT system
in order to e.g. report incidents related to personal data. In addition
appears from the authority's new guidelines for handling
personal data incidents that all incidents must be documented and which ones
information that the documentation must include. The Swedish Data Protection Authority states
that the Ecocrime Agency's procedures for documentation meet the requirements in
the provision in question.

The Swedish Data Protection Authority notes, however, that the authority 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
Datainspektionen's opinion indicates that there is ignorance among employees
about what should be documented. The Swedish Data Protection Authority therefore recommends,
with the support of ch. 5 § 6 BDL, that the Ecocrime Authority implements
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. 15 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 Ecocrime Authority has stated, among other things, following. Information and
training has been provided in the form of e-training, information on the intranet and

information efforts in connection with the new data protection regulation

took effect. The new guidelines for handling personal data incidents

has been implemented and information efforts about this have been carried out.

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

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

The Ecocrime Authority's information security – policy and responsibility (EBMR-A

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

defects and incidents. The guideline states which responsibility employees and

executives have for the authority's information security. Furthermore, have

various guiding documents that have a bearing on the handling of

personal data incidents brought up, e.g. The Ecocrime Authority

guidance for safe handling of information. These are published on

the authority's intranet.

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/

15

Against the background of what appears from the investigation, the Data Protection Authority believes

that the Ecocrime Authority has shown that the authority has provided information

and training on handling personal data incidents to their

coworker.

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 Ecocrime 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.

Miscellaneous

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

The Ecocrime Authority's response was that a negotiation was underway with the Police Authority i

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

Major two. The existence of such an assistance agreement is not covered by this

supervision and therefore the Swedish Data Protection Authority does not take any action in this regard

respect.

This decision has been 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 the attention of:

The Ecocrime 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.