Decision

Diary no

2020-12-17

DI-2019-13115

Your diary no

2019-3082

The Coast Guard

Box 536

371 23 Karlskrona

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

The Coast Guard'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 Coast Guard 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 coast guard should regularly check that the routines for

handling of personal data incidents is followed. Lathund for KEY should

updated and contain information about what is a

personal data incident according to the Criminal Data Act.

3. The coast guard should in the authority's routines for reporting of

personal data incidents specify which data of an occurred

incident to be documented as well as regularly checking that

the procedures for documentation of personal data incidents are followed.

4. The Coast Guard 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 Coast Guard for the purpose of

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 Coast Guard 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 Coast Guard on 4 December

2019 and was followed up with the request for completion on March 4, 2020.

The authority's response to the supervisory letter was received on 17 December 2019 and

the supplement was received on March 23, 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 (Data inspection 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 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 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 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 Coast Guard 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 Coast Guard has carried out

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

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 Coast Guard has essentially stated the following. There isn't anyone

designated function within the authority whose task is to detect

incidents. However, there are several processes to counteract incidents

such as log monitoring, authorization control, technical aids such as

antivirus, web proxy and mail washing. These actions are described in

The Coast Guard's guidelines on information security and guidelines on

personal data processing. Furthermore, it is stated that the authority has procured one

technical system for analyzing events in logs, as in the opinion's

submission not yet implemented. However, manual analyzes are performed

reactive when an incident report has been received by the authority's internal

incident reporting system Key. Regarding organizational measures

it appears from the investigation that the Coast Guard has carried out training and

information efforts regarding information security and processing of

personal data for various professional categories within the authority, which includes

i.a. information on handling personal data incidents.

The Swedish Data Protection Authority can state that the Coast Guard has routines to

detect personal data incidents on the spot.

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 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. To the Coast Guard

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 assessment

The coast guard has, among other things, stated the following. The Coast Guard has procedures for

to report personal data incidents and follows the same internal routine as

other categories within incident reporting. In the Coast Guard's guidelines

on personal data processing dated 2018-05-29 there is a specific section

regarding reporting and routine in the event of personal data incidents. It describes what

a personal data incident can be and how these should be reported.

The authority states that anyone who discovers an incident must urgently

report it in the authority's internal incident reporting system KEY. On

The Coast Guard's intranet also has guidance in the form of a watchdog for

KEY that describes how an incident should be reported. The lazy dog is not

updated since 2014, which is why the personal data incident is not mentioned

specifically. However, personal data incidents are handled in the same way as others

incidents.

Taking into account the submitted documents and what appeared in

case, the Swedish Data Protection Authority states that the Coast Guard from the time

when the Criminal Data Act came into force had and still have routines to deal with

personal data incidents on site. The Swedish Data Protection Authority has, however, previously, i

in connection with a request for prior consultation, recommended

The Coast Guard to update the watchdog for KEY in relation to what

may be considered a personal data incident according to BDL (DI-2018-20352).

The Swedish Data Protection Authority believes that there are reasons to repeat the recommendation.

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

Cape. § 6 BDL, that the Coast Guard regularly checks that the routines for

handling of 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 Coast Guard has essentially stated the following. All
personal data incidents are documented in the authority's internal
incident reporting system KEY from the original report by a reporter
to the manager's actions and investigation during the course of the case. When the investigation is
completed by manager, the Data Protection Officer issues a report from KEY and
diary for the matter, including if the notification has been made to the Data Protection Authority, i
The Coast Guard's document and diary management system Platina.

The Swedish Data Protection Authority states that the Coast Guard has an internal
incident reporting system to e.g. report incidents relating to
personal data. In addition, it appears from the authority's routine at
personal data incidents that all information about incidents must be reported in
the specified system. The Swedish Data Protection Authority notes, however, that the current
the routine lacks a description of which information the documentation must
include.

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 Coast Guard's routines for reporting of personal data incidents are supplemented with a description of which data of an incident that has occurred that must be documented. In addition, should The Coast Guard conduct regular checks of the internal the 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.

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

The Swedish Data Protection Authority's assessment

When asked how information and training about incidents is provided

employees, the Coast Guard has stated i.a. following. The Coast Guard has

carried out targeted information and training initiatives for all staff

regarding the processing of personal data, which includes handling of

personal data incidents. All personnel at the Coast Guard have completed

training on the processing of personal data aimed at everyone

employees must have basic knowledge of treatment of

personal data according to the data protection regulation and the criminal data legislation

as well as an understanding of how personal data should be processed within

Coast Guard operations. The training of the Coast Guard

employees have taken note of internal procedures and guidelines for handling

personal data incidents. The training material covers the basics

education including mandatory knowledge test and a supplementary one

training with in-depth material. Educational material is available via

The Coast Guard's intranet. The Coast Guard plans to during 2020

distribute the training in a digital format with mailing via e-mail to new

coworker. In addition to the interactive training for all staff regarding

personal data processing also has the authority's managers as well

system owners for the authority's various systems participated in a teacher-led training

with information about the authority's regulations regarding information security

and personal data processing. This also included information about

incident management at the Coast Guard as well as

information security-related incidents with other actors.

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

that the Coast Guard has shown that they have provided extensive 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 Coast Guard 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 Coast Guard'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.