Decision

Diary no

2020-12-17

DI-2019-13112

Your diary no

VER 2019-3463

Customs

Box 12854

112 98 Stockholm

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

Customs' 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. Customs should regularly evaluate the effectiveness of the measures taken the security measures to detect personal data incidents and if necessary revise these to maintain adequate protection of personal data.

2. Customs should review the agency's routines for logging and log follow-up and update these as applicable criminal data legislation.

3. The Customs Service should draw up a consolidated document with written guidelines or procedures for handling personal data incidents.

4. Customs should regularly check that the procedures for handling personal data incidents are followed.

5. The customs office should in the authority's routines for handling 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.

6. Customs should provide its employees with ongoing information and
recurrent training in the handling of personal data incidents
and about the reporting obligation.

The Swedish Data Protection Authority closes the case.

Account of the supervisory matter

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

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

personal data incident can be, for example, that personal data has been sent to the wrong recipient, that access to the personal data has been lost, that computer equipment that stores personal data has been lost or stolen, that someone inside or outside the organization accesses information like that lacks authorization to.

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

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on that free flow of such data and on the repeal of Directive 95/46/EC (general data protection regulation).

2 A competent authority is according to ch. 1 § 6 BDL an authority that processes personal data for the purpose of preventing, preventing or detecting criminal activity, investigate or prosecuting offences, enforcing criminal penalties or maintaining public order and security.

3 Prop.2017/18:232 p. 438

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

There can be many reasons why a personal data incident occurs. Of Datainspektionen's report series Reported personal data incidents under period May 2018 - December 2019 it appears that the most common causes

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

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

The Data Inspectorate has initiated this supervisory case against the Swedish Customs Administration with the aim of

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 (BDL). IN

the review also includes checking whether the Swedish Customs Administration 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 Customs Board on 4 December 2019 and

was followed up with a request for completion on March 4, 2020. The authority's

response to the supervisory letter was received on 17 January 2020 and the supplement

received on March 19, 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.

4

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, scope, 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 that is processed is.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 charges 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 Data Inspectorate has to take a position on the Swedish Customs Service

has documented procedures for detecting personal data incidents according to

the Criminal Data Act and whether the authority has and has had routines to deal with it

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 Data Inspectorate must take a position on whether the Swedish Customs Administration has carried out

information and training efforts for its employees with a focus on

handling of personal data incidents according to BDL.

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.

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 Swedish Customs Service has essentially stated the following. The authority has detailed routines and guidelines for monitoring the processing of personal data i Customs' IT system for law enforcement activities. By logging and systematic log follow-up, the Swedish Customs Service can detect unauthorized persons activity in their IT systems. On the authority's intranet there is information about i.a. the security logging and how the follow-up of the security logging goes to. In the Customs' supplementary response, reference is made to the authority's internal rule on follow-up of processing of personal data in the Swedish Customs Administration's IT system for law enforcement activities (STY 2015-99) and to the authority supporting documents for Guidance on follow-up treatment of personal data in the Swedish Customs Service's IT system for law enforcement activities (VER 2015-489) submitted. It also appears that technical solutions for to counter and detect IT and information security incidents, including personal data incidents, is protection against malicious code on clients (servers and workstations), next-generation firewalls to detect threats in the network and SIEM solution13 to analyze threats in networks and IT systems.

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 A SIEM solution collects log data from the network, extracts meaningful information from the logs, compare different events to discover attack patterns and help search log data for root cause analysis, something that provides in-depth insight into what is happening in the network.

As far as mobile phones are concerned, these are handled by security software that meets Customs' requirements for handling information of high security value. Security software can, for example, identify malicious behavior on mobile phones such as improper access to data and take various measures depending on the dignity of the wrong. Examples of measures can be locking out from internal applications, selective deletion of internal data or factory reset. Regarding organizational measures, please refer to the Swedish Customs Administration to the authority's governing document STY 2019-273, Internal rule for business protection, in which i.a. states that if a service card or IT equipment is lost or has been used by someone else, this must be reported urgently to IT support. After that, the IT security function must immediately be informed. The investigation shows that the Swedish Customs Service has carried out training and information efforts. All employees must undergo a mandatory online introductory course on personal data processing which includes information on personal data incidents and reporting obligations.

The Data Inspectorate can state that the Swedish Customs Service has routines for detection personal data incidents on site. The Swedish Data Protection Authority notes, however, that they documents relating to logging and log follow-up referred to by the Swedish Customs Administration to, i.e. The authority's intranet, STY 2015-99 and VER 2015-489, is based on Personal Data Act (1998:204) and has not been updated in accordance with current regulations data protection legislation for law enforcement. The Swedish Data Protection Authority believes that this justifies a review of these procedures.

The Swedish Data Protection Authority therefore recommends, with the support of ch. 5. § 6 BDL, that

The Swedish Customs Service reviews the authority's routines for logging and log follow-up
and updates these in accordance with current data protection legislation for
law enforcement activities.

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 for the Swedish Customs Service to
be able to maintain a sufficient level of protection of personal data over time
recommends the Data Inspectorate, with the support of ch. 5. § 6 BDL, that
the authority regularly evaluates the effectiveness of those taken
the security measures to detect personal data incidents and that
the authority updates these if necessary.

Procedures for handling personal data incidents

In order to live up to the requirements for organizational measures in ch. 3. Section 8
BDL, the personal data controller must have documented internal routines that
describes the process to be followed when an incident has been detected or
occurred, including how the incident will be contained, managed and recovered,
as well as how the risk assessment should be carried out and how the incident should be reported internally
and to the Swedish Data Protection Authority. The routines must include, among other things, what a
personal data incident is/can be, when an incident needs to be reported, and
to whom, what must be documented, the distribution of responsibilities and which
information that should be provided within the framework of notification to
The Swedish Data Protection Authority.

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

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

i.e. on August 1, 2018.

The Swedish Data Protection Authority's assessment

The Customs Office has, among other things, stated the following. The authority has routines/guidelines for

to report personal data incidents and information about this can be found at

the authority's intranet. Information on the intranet shows that

personal data incidents are categorized as a

information security incident which should be reported to IT support for

assessment and further handling. Customs has also submitted

the authority's temporary routine for handling personal data incidents

dated 2019-04-29 as well as a description of how IT support should register

reported personal data incidents. In the Swedish Customs Service's supplementary response

the authority has made it clear that similar temporary routines for handling

personal data incidents were already in place in April 2018 and that these

was updated in April 2019. Any further update of the routines has

not happened since then. Customs also states that there is nothing

produced guidance document that specifically addresses personal data incidents

and refers to the authority's governing document STY 2019-785 which contains

a routine for handling information and IT security-related incidents

and problems. In cases where personal data is affected in an incident,

the incident according to the steering document is reported via IT support.

Taking into account the submitted documents and what appeared in

the case, the Data Inspectorate states at the outset that the Customs Agency from

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

handle personal data incidents on site. From the review, however, it has emerged that the Customs Office's routines are found in various documents and contain different parts of the routines. For example, it appears from the Customs Agency's intranet information about what a personal data incident is and how an incident should be are reported and in the authority's temporary procedures for handling of personal data incidents, it is possible to read about the division of responsibility and the process for handling personal data incidents. The Swedish Data Protection Authority also notes that the Swedish Customs Administration lacks a produced guidance document specifically for handling personal data incidents. It can according to Datainspektionen's opinion implies a problem with dispersed information and risk of slow incident handling.

The Swedish Data Protection Authority therefore recommends, with the support of ch. 5. § 6 BDL, that Customs prepares a consolidated document with written guidelines or procedures for handling personal data incidents.

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 Customs Agency 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 Swedish Customs Service has essentially stated the following. A case, such as a

personal data incident, is documented in JIRA Service desk. The report on

the investigation of a personal data incident is saved. External communication with

The Data Inspectorate is saved in the diary under diary series VER. Of the authority

intranet, it appears that the Swedish Customs Service must document everyone

personal data incidents and at the same time a description of which appears

details and circumstances of a personal data incident which

the documentation must include. Customs has also developed a template for

reporting and investigation of personal data incidents where it appears a

detailed description of an incident that occurred and what to do

be documented. The template is intended to serve as a support during the investigation

and as an internal documentation when the investigation is completed.

The Data Inspectorate states that the Swedish Customs Service has an internal IT system to

i.a. report incidents related to personal data. In addition, it appears from

the authority's intranet that all personal data incidents must be documented

as well as what information the documentation must cover. In addition, have

the authority has produced a template for reporting and investigation of

personal data incidents that meet the requirements of the current

the provision. The Data Inspectorate notes, however, that the Customs Agency's routines for

handling of personal data incidents lacks a description of which

information that 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 Customs' routines for handling of personal data incidents are supplemented with a description of which data of an incident that has occurred that must be documented. In addition, the Customs Service should carry out 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. 14 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 Swedish Customs Administration has stated i.a. following. Customs uses the tool
Teacher platform where employees can complete online courses. All
employees must complete a mandatory web-based introductory course on
personal data processing. The course component includes, among other things, training on
what constitutes a personal data incident and how it should be reported
internal. Information on what constitutes personal data incidents and if
the importance of reporting these is also included as part of it
basic training that customs aspirants in law enforcement undergo.
Furthermore, the Swedish Customs Administration has plans for further information initiatives that will
be directed to specific business areas.
Against the background of what appears from the investigation, the Data Protection Authority believes
that the Swedish Customs Service has shown that the authority has provided information and training
on the handling of 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 Customs Agency provides the employees with ongoing information

and recurring training in the handling of personal data incidents

and the obligation to report these.

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/

14

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 Swedish Customs Service'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.