Decision

Diarienr

2020-12-17

DI-2019-13112

Ert diarienr

VER 2019-3463

The Swedish Customs

Box 12854

112 98 Stockholm

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

The Swedish Customs' routines for handling

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 Swedish Customs should regularly evaluate the effectiveness of those taken

security measures to detect personal data incidents and

revise these if necessary to maintain adequate protection of

personal data.

2. The Swedish Customs should review the authority's routines for logging and

log follow-up and update these in accordance with current

criminal data legislation.

3. The Swedish Customs should draw up a single document with written guidelines

or routines for handling personal data incidents.

4. The Swedish Customs should regularly check the procedures for handling

personal data incidents are followed.

5. The Swedish Customs should in the authority's routines for handling

personal data incidents specify which data of a occurred

incident to be documented and regularly check that

the procedures for documentation of personal data incidents are followed.

6. The Swedish Customs 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

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 Customs with the aim of
check if 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 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 Customs on 4 December 2019 and
was followed up with a request for supplementation on 4 March 2020
response to the supervisory letter was received on 17 January 2020 and the supplement
received on March 19, 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 the decision

The Data Inspectorate's review

In this supervisory matter, the Data Inspectorate has to take a position on the Swedish Customs

has documented routines for detecting personal data incidents according to

the Criminal Data Act and whether the authority has and has had routines for dealing with it

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 Customs has implemented

information and training initiatives for its employees with a focus on

handling of personal data incidents according to BDL.

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.

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 Swedish Customs has mainly stated the following. The authority has detailed routines and guidelines for following up the processing of personal data in The Swedish Customs' IT system for law enforcement activities. Through logging and systematic log monitoring, the Swedish Customs can detect unauthorized persons activity in their IT systems. Information about the authority's intranet is available i.a. security logging and how the security logging is followed up to. The Swedish Customs' supplementary answer refers to the authority's internal rule on follow-up of processing of personal data in the Swedish Customs' IT system for law enforcement activities (STY 2015-99) and to the authority supporting document for Guidance on follow-up of treatment of personal data in the Swedish Customs' 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 work computers), next-generation firewalls to detect threats in the network and SIEM solution13 to analyze threats in networks and IT systems.

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 A SIEM solution collects log data from the network, extracts meaningful information from logs, compares different events to detect attack patterns and helps search log data for causal analysis, which provides an in-depth insight into what is happening in the network.

As far as mobile phones are concerned, these are handled by security software that complies

The Swedish Customs' requirements for handling information of high protection value.

Security programs can, for example, identify harmful behaviors on

mobile phones such as unauthorized access to data and taking various actions

depending on the dignity of the error. Examples of measures can be lockout

from internal applications, selective deletion of internal data or

factory reset. Regarding organizational measures, the Swedish Customs refers

to the authority's governing document STY 2019-273, Internal rule for

operational protection, in which i.a. states that if a service card or IT equipment has been lost or has been used by someone else, this must be reported

urgently to IT support. After that, the IT security function should be immediate

informed. The investigation shows that the Swedish Customs has carried out training and information initiatives. 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 has routines for detecting

personal data incidents on site. The Data Inspectorate notes, however, that they

documents regarding logging and log follow-up that the Swedish Customs refers

to, i.e. the authority's intranet, STY 2015-99 and VER 2015-489, is based on

the Personal Data Act (1998: 204) and has not been updated in accordance with current law

data protection legislation for law enforcement activities. The Data Inspectorate

considers that this justifies a review of these procedures.

The Data Inspectorate therefore recommends, with the support of ch. § 6 BDL, att

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

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

Routines for handling personal data incidents

In order to be able to live up to the requirements for organizational measures in ch. § 8
BDL, the person responsible for personal data must have documented internal routines such as
describes the process to be followed when an incident has been detected or
occurred, including how to limit, manage and recover the incident,
and how the risk assessment is to be carried out and how the incident is to be reported internally
and to the Data Inspectorate. The routines must state, among other things: 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 Swedish Customs has i.a. stated the following. The authority has routines / guidelines for

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

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

personal data incidents are categorized as one

information security incident which must be reported to IT support for

assessment and further handling. The Swedish Customs has also submitted

the authority's temporary routine for handling personal data incidents

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

reported personal data incidents. In the Swedish Customs' supplementary answer

the authority has clarified that similar temporary routines for handling

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

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

has not happened since. The Swedish Customs also states that there is nothing

produced control documents that specifically address 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 shall

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

Taking into account the documents submitted and what has emerged in

In the case, the Data Inspectorate initially states that the Swedish Customs from

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

handle personal data incidents on site. Of the review, however, it has
it has emerged that the Swedish Customs' routines are found in various documents and contain
different parts of the routines. For example, the Swedish Customs' intranet shows
information about what a personal data incident is and how an incident should be
reported and in the authority's temporary routines for handling
personal data incidents, you can read about the division of responsibilities and
the process for handling personal data incidents. The Data Inspectorate
also notes that the Swedish Customs lacks a produced control document
specifically for handling personal data incidents. It can according to
The Data Inspectorate's opinion entails a problem with disseminated information
and risk of slow incident management.

The Data Inspectorate therefore recommends, with the support of ch. § 6 BDL, att
The Swedish Customs prepares a single document with written guidelines or
routines for handling personal data incidents.

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 Swedish Customs regularly checks that the routines for
handling of personal data incidents is 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 Swedish Customs has mainly stated the following. A case, such as one

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

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

The data inspection is saved in the diary during the diary series VER. By the authority

intranet states that the Swedish Customs must document everyone

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

information and circumstances of a personal data incident which

the documentation shall include. The Swedish Customs has also produced a template for

reporting and investigation of personal data incidents where one appears

detailed description of an incident that occurred and what to do

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

and as an internal documentation when the investigation is completed.

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

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

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

and what information the documentation must include. In addition,

the authority has developed 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 Swedish Customs' routines for

handling of personal data incidents lacks a description of which

information that the documentation must include.

To be able to document occurred personal data incidents correctly

and thereby counteract the risk of the documentation becoming deficient or

incomplete is important. Inadequate documentation can lead to

the incidents are not handled and remedied properly, which can get

impact on privacy protection. The Data Inspectorate therefore recommends,

with the support of ch. 5 § 6 BDL, that the Swedish Customs' routines for handling

personal data incidents are supplemented with a description of which data

of an incident that is to be documented. In addition, the Swedish Customs should

carry out regular checks on 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. 14 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 Customs has stated i.a. following. The Swedish Customs uses the tool

Teacher platform where employees can complete online courses. All

employees must undergo a mandatory online 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

internally. Information on what constitutes personal data incidents and on

the importance of reporting these is also part of it

basic training undergone by customs graduates in law enforcement.

Furthermore, the Swedish Customs has plans for further information efforts that will

be aimed at specific areas of activity.

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

that the Swedish Customs 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 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 Swedish Customs 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. 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/

14

This decision was made by unit manager Charlotte Waller Dahlberg after

presentation by lawyer Maria Angelica Westerberg. At the final

The IT security specialist Ulrika also handles the case

Sundling and the lawyer Jonas Agnvall participated.

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

Copy for information to:

The Swedish Customs' data protection representative

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

on 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.