Decision

Diarienr

2020-12-17

DI-2019-13114

Ert diarienr

8-3407

The Swedish Tax Agency

Unit 6800

171 94 Solna

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

The Swedish Tax Agency's routines for handling

personal data incidents

Table of Contents

The Data Inspectorate's decision 2

Report on the supervisory matter 3

Applicable provisions 4

Grounds for the decision 6

The Data Inspectorate's review 6

Procedures for detecting personal data incidents 7

The Data Inspectorate's assessment 8

Routines for handling personal data incidents 9

The Data Inspectorate's assessment 9

Procedures for documentation of personal data incidents 10

The Data Inspectorate's assessment 11

Information and training on personal data incidents 11

The Data Inspectorate's assessment 12

How to appeal..... 14

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 Tax Agency 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 tax authority should regularly check the procedures for handling

of personal data incidents are followed.

3. The Swedish Tax Agency should regularly check that the internal routines for

documentation of personal data incidents is followed.

4. The Swedish Tax Agency 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.

DI-2019-13114

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 Tax Agency 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 incidents according to the Criminal Data Act. The review also includes that

check whether the Swedish Tax Agency has routines for documenting incidents

which meets the requirements of the Criminal Data Regulation (BDF) and if

the authority has carried out information and training initiatives on

personal data incidents.

The audit began with a letter to the Swedish Tax Agency on 4 December 2019

and was followed up with a request for completion on 4 March 2020.

The authority's response to the supervisory letter was received on 27 January 2020 and

the supplement was received on March 25, 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 a position to decide on

The Swedish Tax Agency has documented routines for detecting

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

documentation of incidents in ch. 3 14 § BDF. In addition,

The Data Inspectorate will decide whether the Swedish Tax Agency has implemented

Prop. 2017/18: 232 pp. 198

Liability for violations is strict. Thus, neither intent nor negligence is required to

it must be possible to charge a penalty fee, see bill. 2017/18: 232 pp. 481.

8

9

information and training initiatives for its employees with a focus on

handling of personal data incidents according to BDL.

The review does not include the content of the routines or training efforts

but is focused on verifying that the reviewing authority has

routines on site and that it has implemented training initiatives for

employees regarding personal data incidents. The review includes

however, if the authority's routines contain instructions to document them

information required by the Criminal Data Regulation.

Routines for detecting personal data incidents

The personal data that competent authorities handle within the framework of their

law enforcement and crime investigation activities are to a large extent of

sensitive and privacy sensitive nature. The nature of the business is high

requirements on the ability of law enforcement agencies to protect them

information was registered through the necessary protection measures to e.g.

prevent an incident from occurring.

The obligation to report personal data incidents according to ch. 9 § BDL

shall be construed in the light of the general requirements to take appropriate technical and

organizational measures, to ensure appropriate security for

personal data, which is prescribed in ch. 2 and 8 §§. An ability to fast

Detecting and reporting an incident is a key factor. Because they

law enforcement agencies must be able to live up to

the reporting requirement, they must have internal routines and technical capabilities for

to detect an incident.

Based on the needs of the business and with the support of risk and vulnerability analyzes

competent authorities can identify the areas where there is a greater risk

that an incident may occur. Based on the analyzes, the authorities can then

use various instruments to detect a security threat. These can be

both technical and organizational measures. The starting point is that they

the safety measures taken must provide adequate protection and that incidents do not

should occur.

Examples of technical measures include intrusion detectors as automatic

analyzes and detects data breaches and the use of

log analysis tool to detect unauthorized access

(log deviations). An increased insight into the business' "normal" network

traffic patterns help to identify things that deviate from the normal

the traffic picture towards, for example, servers, applications or data files.

Organizational measures can, for example, be the adoption of internal strategies

for data protection relating to internal rules, guidelines, routines and different types of

governing documents and policy documents.10 Guidelines and rules for handling

personal data, routines for incident management and log follow-up11 constitute

examples of such strategies. Periodic follow-up of assigned

authorizations is another example of organizational measures. In a competent

authority, there shall be procedures for allocation, change, removal and

regular verification of privileges.12 Information and training of

staff on the rules and routines for incident management to be followed

also examples of such measures.

The Data Inspectorate's assessment

The Swedish Tax Agency has mainly stated the following. The personal data incidents

which is discovered and reported is based on the individual manager and

the employee is observant and has the ability and knowledge to be able to

identify a suspected personal data incident. All managers and

employees have a responsibility to report suspects

personal data incidents. Information about what could be a suspect

personal data incident has been communicated to all managers and

employees at the tax crime unit (SBE). The Swedish Tax Agency further states that

the authority has implemented organizational and technical routines such as

log follow-up and authorization assignment. In terms of technical solutions

states that the central computer systems for the administrators of the tax crime unit

is the Swedish Tax Agency's criminal investigation support (RIF BU) for the criminal investigator

operations (the pre-investigation operation) and the Swedish Tax Agency

intelligence register (SKUR) for the intelligence activities. RIF BU is

built and designed in such a way that it has a number of technical routines

to counteract personal data incidents. Regarding organizational

measures state that access to information and permissions is controlled

through the use of various access control systems and access cards.

The access control system has registers of all users and theirs

authorizations and transactions against the system being continuously checked against

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

the register. In addition, during 2018-2019, the Swedish Tax Agency has trained and

informed employees and managers within the tax crime unit in

data protection issues. All employees have received information especially about e.g.

how a personal data incident is to be reported and what support is available for

to report and assess personal data incidents.

The Data Inspectorate can state that the Swedish Tax Agency has routines for

detect personal data incidents on site.

The obligation to take precautionary measures to detect

personal data incidents are not linked to a specific time but the measures

shall be continuously reviewed and, if necessary, changed. For the Swedish Tax Agency 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 e.g. what a

personal data incident is / can be, when an incident needs to be reported, and

to whom, what is to be documented, the division of responsibilities and which

information that should be provided in the context of notification to

The Data Inspectorate.

The Data Inspectorate's control of routines for handling

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

i.e. on August 1, 2018.

The Data Inspectorate's assessment

The Swedish Tax Agency has i.a. stated the following. The authority has routines / guidelines

to report and manage detected personal data incidents. The boss

or employees who discover a suspected personal data incident within

SBE must report this in the Swedish Tax Agency's User Support or the IT portal via

one

e-service. SBE has its own entrance in User Support and the IT portal called

"Personal data incident according to the Criminal Data Act (SBE)". The Swedish Tax Agency has i.a.

submitted Routine personal data incidents dated 2019-05-09 and

Complementary internal routine at SBE for reporting of

personal data incidents dated 2019-08-13 that supplement it

the former routine. The Swedish Tax Agency states that the authority's routine

personal data incidents are primarily developed for the Data Protection Regulation,

but also takes into account BDL and BDF. The Swedish Tax Agency further states that

the authority in May 2018 established a support to identify, report,

assess and manage personal data incidents (Report 2018-05-18

Data Protection Ordinance Managing Personal Data Incidents). The report

intended to support the Swedish Tax Agency's activities in the event of personal data incidents

in accordance with the Data Protection Regulation and to support the activities of

the tax crime unit in the event of personal data incidents according to the Criminal Data Act.

On 26 November 2018, the Swedish Tax Agency adopted the document Routine

personal data incidents (updated on 9 May 2019 and 30 respectively

December 2019). The Swedish Tax Agency states that there were special routines / guidelines for handling personal data incidents and a digital management system for reported personal data incidents on site when BDL came into force August 1, 2018.

Taking into account the documents submitted and what has emerged in the case, the Data Inspectorate states that the Tax Agency from the time then the Criminal Data Act came into force has had and has routines for dealing with personal data incidents on site.

To be able to handle discovered personal data incidents in a correct way and counteract its effects and risks on the data subjects' personalities Integrity is important. The Data Inspectorate therefore recommends, with the support of Chapter 5 § 6 BDL, that the Tax Agency 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 Tax Agency has mainly stated the following. It is

the responsibility of the personal data coordinators (PU-IK) that the reports become recorded, processed and documented. It is further stated that in support of processing and documentation of reported personal data incidents there is a digital management system where all measures taken documented. There are also supporting documents for record keeping of personal data incidents. Of the authority's Routine personal data incidents as well as their Complementary internal routine at SBE for reporting by personal data incidents it appears that all personal data incidents must documented. The documentation must state the circumstances surrounding it the personal data incident, its effects and the measures taken occasion of it.

The Data Inspectorate states that the Swedish Tax Agency has an internal IT system for to report personal data incidents. In addition, it appears from the submitted the routines that all personal data incidents must be documented and that has specified which information the documentation must include.

The Data Inspectorate states that the Swedish Tax Agency's routines for documentation meets the requirements of the relevant provision.

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 Tax Agency implements regular controls of the internal documentation of personal data incidents.

Information and education about personal data incidents

The staff is an important resource in the security work. It's not just enough

internal procedures, rules or governing documents if users do not follow them.

All users must understand that the handling of personal data must take place in one go
legally secure and that it is more serious not to report an incident than

to report e.g. a mistake or a mistake. It is therefore required that everyone
users receive adequate training and clear information on data protection.

The person responsible for personal data must inform and train his staff in matters
on data protection including the handling of personal data incidents. Of
The Swedish Data Inspectorate's report series Reported Personal Data Incidents under
in the period 2018-2019, it appears that the human factor is the most common
the cause of reported personal data incidents. 13 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 Tax Agency has stated i.a. following. The Swedish Tax Agency has internal
training in data protection for employees and managers. The Swedish Tax Agency has
trained and informed all employees and managers within SBE through

that during 2018-2019 they have undergone the Swedish Tax Agency's training in

data protection issues. During the spring / summer of 2018, the employees took part

of educational films produced by the Swedish Environmental Crime Agency about

the data protection reform, including the Criminal Data Act. In addition, they have received

information on the Data Protection Regulation and the Criminal Data Act, in particular on

reporting of personal data incidents. Section heads have also left

information to all employees that personal data incidents should

reported, how to proceed to report as well as what may be one

personal data incident. All managers at SBE have received information from

The Swedish Tax Agency's data protection representative. Every manager and employee has completed

a basic digital course on the Data Protection Regulation, which includes about two

hours of self-study.

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/

13

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

that the Swedish Tax Agency has shown that the authority has provided information and

training on the handling of personal data incidents to their 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 Tax Agency provides employees with ongoing information

and recurring training in the handling of personal data incidents

and the obligation to report these.

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 Tax Agency's 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

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.