Customs

Sent by email only

Diary number:

DI-2020-5868

Your diary number:

VER 2020-933

Date:

2022-03-14

Decision after supervision according to

the crime data act - Customs

personal data processing on

service mobiles

The Privacy Protection Authority's decision

The Privacy Protection Authority notes that the Swedish Customs Service has processed personal data

contrary to ch. 3 Sections 2 and 8 of the Crime Data Act (2018:1177), BDL, by

unknown time until November 8, 2019 not having taken sufficient technical and

organizational measures to ensure and be able to demonstrate that

the personal data processing was constitutional and to protect the personal data

that was processed on office mobiles from being copied and stored in a cloud service.

The Privacy Protection Authority decides with the support of ch. 6. § 1 BDL that the Customs Agency shall

pay a sanction fee of 300,000 (three hundred thousand) kroner.

Account of the supervisory matter

On November 8, 2019, the Swedish Privacy Agency (IMY) received a notification about

personal data incident according to BDL from the Swedish Customs Administration. The application was completed on 14 and

15 November 2019 and 11 December 2019. The incident report showed that

employees have been able to use company mobile phones in a way that was not permitted. It was

question about the use of a program that resulted in personal data that

was processed according to BDL was stored in a cloud service and thereby spread on a

unauthorized manner. In light of the information in the notification, IMY decided to initiate a

review of what caused the described personal data incident and which

measures taken by the Swedish Customs Service to avoid similar incidents from happening again.

During the inspection, the Swedish Customs Administration has answered a number of questions, and the Swedish Customs Service's answers are as follows

essentially the following. Two employees at the Swedish Customs Service's customs crime operations have

used the Google Photo cloud service in their company mobile phones. The officials had connected

their private Google Photos accounts to their work mobiles which automatically synced them

the service-related recordings to the cloud storage function. The officials must

is considered to have inadvertently disclosed any personal data belonging to individuals who have been

subject to criminal suspicion or included in criminal investigations by taking photographs and

movies taken on the service have ended up in the software that stores information in the cloud.

When employees discovered that these work-related recordings were stored in

the cloud, they have been continuously deleted from the account that was linked to the service mobile phone.

Mailing address:

Box 8114

104 20 Stockholm

Website:

www.imy.se

E-mail:

imy@imy.se

Phone:

08-657 61 00

It happened even before the reported personal data incident was discovered.

The use of the current service was not permitted. The customs authority's assessment is that the risk that the personal data has been spread is low because the data has been found on password-protected accounts with Google.

In connection with the incident, the business stopped the use of the cloud service via message on 8 November 2019 to responsible managers and employees within department that the service may not be used. On 20 November 2019, a new one was introduced protective measure for the company mobile where the ability to download applications from App Store was blocked and all applications that could contain vulnerabilities was uninstalled from the service mobiles. Only applications distributed via Customs' EMM platform (Enterprise Mobility Management) is currently available in employees' company mobiles. Introduction of new applications for the service mobile phones is now handled according to a special routine. Information on how the service mobiles get used has been communicated to employees in the Swedish Customs Administration again.

The Swedish Customs Administration conducts continuous work with security and integrity issues. In this work includes continuously evaluating existing security measures, both technical and organizational, and to, if necessary, adjust and update them in relation to the risks for the authority's IT security and the rights of data subjects. A large part of the Customs Office employees are in need of applications in the office mobile to be able to carry out their work duties. To completely prohibit the use of applications has for this reason not been possible. Mobile and app security is and has been an area of focus for Customs. For security reasons, a change of mobile provider was carried out in 2017.

Functionality in some applications has also been limited or disabled. During
in the fall of 2019, it was announced that a major escalation of
the mobile protection which meant that available applications for download were restricted
and that existing applications that did not meet the requirements of the Swedish Customs Administration were deleted. The
enhanced mobile protection would enter into force on 11 November 2019. Even before this
however, the Customs' IT department had done work to reduce the number
applications on employees' work mobile phones. In that work was limited
applications that had too few users or were found to be clearly malicious.
Google Photos had been downloaded before the ability to download applications
was restricted. For the Swedish Customs Service's crime-fighting activities - within which it
the incident in question occurred - however, there were instructions to only approved
applications and other data media were allowed to be used in the service.
Admittedly, the Swedish Customs Administration has not immediately blocked the download of applications from
App Store in connection with the service mobile phones being replaced, but the authority has
continuously evaluated risks with the use of applications and quickly escalated
up limitations in the use of these in connection with existing
safety measures followed up.
The Swedish Customs Administration has also taken organizational measures to protect the personal data
which is processed in the business. The Swedish Customs Service has, among other things, produced guidelines,
conducted trainings, published information on the intranet and established conditions for
use of mobile devices to increase employee awareness around
information security issues in general, and the use of service mobile phones and
cloud services in particular. To be able to start using a company mobile as an employee in
Customs requires that you read and approve a text. The text states, among other things, to
information that belongs to the Customs Service may only be handled and stored in the Customs Service
information system, or in IT equipment or peripherals that have been approved by

2018-132, which is also included in the Swedish Customs Administration's introductory training. Similar information about how the service mobile can be used has also been published on the Swedish Customs Administration's intranet. Current use of applications states, for example, that internal and/or protected information should never be handled in applications and/or services not provided by Customs. Furthermore, employees have been warned in articles published on the intranet that use of certain downloaded applications may result in the information not longer is private as many applications and services store information in the cloud.

Employees are also reminded to take the information classification into account when downloading or uses applications because it can have a direct impact on the Swedish Customs Administration information security. Employees who do not have knowledge of what happens when downloading a certain application to their mobile device is also recommended to refrain from such downloads.

Given that the recordings that led to the notification of the personal data incident has been deleted, it is not possible to specify which or how many people may have been affected. For that reason, the Swedish Customs Administration has deemed it impossible to inform any touched people.

In the matter, the Customs Service has submitted internal documents that regulate the use of mobile communication devices, including the authority's guidelines for handling information in company mobiles and information about telephone usage published on the intranet before and after the incident, as well as course plans for education in information security, business protection and personal data processing.

Justification of the decision

The Swedish Customs Service is responsible for personal data for how employees

processes personal data on company mobile phones

According to ch. 3, the customs office is § 1 BDL and ch. 1 Section 3 of the Act (2018:1694) on Customs

processing of personal data within the scope of the Criminal Data Act (Customs

criminal data act) personal data controller for all processing of personal data that is carried out

under the direction of the authority or on behalf of the authority. This means that the Swedish Customs Service

is responsible for the personal data processing that employees of the Swedish Customs Administration carry out within

the area of the Criminal Data Act,1 for example the processing that takes place to prevent,

prevent or detect criminal activity. As part of that responsibility needs

Among other things, the Swedish Customs Service ensures that appropriate technical and organizational measures are taken

to ensure and demonstrate that the authority's personal data processing is

constitutional and to protect the personal data that is processed. It needs more

examples include clear procedures and guidelines for employees' use of company mobile phones

and the employees also need to receive training and information about how personal data

may be processed on the telephones.

The customs office has stated that the use of Google Photos was not allowed within

the authority. However, the employees have used the program on company mobile phones when they

performed their duties at the authority. The fact that the use of

Google Photo was not permitted does not absolve the Swedish Customs Administration of the responsibility that the authority

has as

personal data controller. Against this background, the Customs Service is responsible for it

processing that the employees have carried out in connection with the use of Google

Photo.

1 Prop. 2017/18:232 pp. 171 f., 319 and 452 f.

Customs must take appropriate technical and organizational measures

measures to protect the information on company mobile phones

The investigation shows that the Swedish Customs Service, through the use of the Google Photo application, has processed an unknown number of personal data from the law enforcement activities in a cloud service. As the Swedish Customs Service notes, the authority has when using the cloud service inadvertently disclosed personal data belonging to individuals who were subject to criminal suspicions or involved in criminal investigations.

As a personal data controller, the Swedish Customs Administration has according to ch. 3 § 2 BDL an obligation to, through appropriate technical and organizational measures, ensure and be able to demonstrate that the authority's processing of personal data is constitutional and that it data subject's rights are protected. This means, among other things, measures in the form of adopting internal strategies for data protection, to inform and train staff and ensure technical traceability through logging and log follow-up. 2 of 3 ch. § 1 the crime data regulation (2018:1202), BDF, it appears that the technical and organizational measures that the personal data controller must take must be reasonable with regard to the nature, scope, context and purpose of the processing and the special risks with the treatment.

According to ch. 3, the Customs § 8 BDL also take appropriate technical and organizational measures measures to protect the personal data processed, especially against unauthorized or unauthorized processing and against loss, destruction or other accidental damage. Such measures can, for example, be training in data security and information about the importance of that the following applicable security procedures.3 The security measures must according to ch. 3 Section 11 BDF achieve a level of protection that is suitable with regard to, among other things

the nature, scope, context and purpose of the processing, the particular risks involved

the processing and how privacy-sensitive the personal data that is processed is.

When personal data is handled on mobile communication devices, e.g. a service mobile,

there are significant risks of personal data being spread unintentionally. In order to

the security level must be considered sufficient because it is required that there are well-thought-out

written instructions for this type of handling.4 There must also be a

awareness within the organization that the processing of privacy-sensitive data

in mobile devices can involve certain special risks that can have severe consequences

for those whose personal data is at risk of being disseminated. It can be used on a company mobile phone

different types of services and download applications that may affect security and

entail accidental dissemination of personal data.5 That a company mobile can also

used for private use further entails a risk of confusion between

work-related and private material.

It is part of the nature of the matter that the information the Swedish Customs Administration handles according to BDL and

Customs' crime data act is often sensitive to privacy. Information about crime or suspicion

if crimes are examples of such categories of personal data that are special

privacy sensitive. Such information is also often covered by confidentiality, for example

according to ch. 35 Section 1 of the Publicity and Confidentiality Act (2009:400). Pictures and movies like

handled within the framework of law enforcement activities can in itself be a lot

privacy sensitive.

2 See prop. 2017/18:232 p. 453

3 See prop. 2017/18:232 p. 457 f.

4 Cf. IMY's decision of 26 November 2013 (279-2013) and IMY's decision of 30 January 2014 (280-2013).

5 Cf. IMY's decision of 8 May 2013 (1552-2012).

When privacy-sensitive data is processed on a service mobile, which means special
risks from an integrity point of view, as stated above clear guidelines are required as well
well thought out and well implemented written instructions to avoid that
privacy-sensitive and confidential information is inadvertently disseminated. In addition, must
technical measures are taken to limit the risk of the instructions not being followed.
The information that was on the Customs Agency's intranet before the incident was certainly relevant
risks that exist when using applications, e.g. that images may be stored
both in the mobile phone and in the cloud. The instruction stated, among other things, that internal or
protected information should never be handled in applications not provided by
Customs and that users should wait before downloading an application about this
is doubtful about what information the application collects. In the instructions were left
however, not any detailed information about which applications are allowed to load
down or information on restrictions for private use.6 Nor otherwise have
The customs authority has shown that the authority provided such information to the employees before
the incident. Nor has there been any technical limitation on which applications
which could be downloaded.
Overall, IMY assesses the technical and organizational measures taken
before the incident in question were not sufficient for the Customs Agency to be considered to have complied
the requirements in ch. 3 §§ 2 and 8 BDL on ensuring and being able to demonstrate that
the personal data processing was constitutional and to protect
the personal data from unauthorized or unauthorized processing. Customs has therefore
violated these regulations.
IMY notes that, after the incident occurred, the Swedish Customs Administration has clarified its guidelines for
handling of information in company mobiles and has developed new routines for introduction

of new applications and introduced technical limitations regarding which applications are

can be used in the service.

Choice of intervention

In ch. 5 § 7 BDL specifies the corrective powers IMY can use in

violations of said law. These consist of, among other things, injunctions, prohibitions against

processing and issuance of a penalty fee.

According to ch. 6 §§ 1 and 2 BDL, IMY can issue a penalty fee in case of violation of

otherwise the provisions in ch. 3. §§ 2 and 8 BDL. The penalty fee must meet the requirements

which is stated in Article 57 of the Criminal Data Directive7 that sanctions must be proportionate,

deterrent and effective. Of ch. 6 Section 3 second paragraph BDL follows that for a

violation of ch. 3 §§ 2 and 8 BDL, a sanction fee may amount to a maximum of ten

million kroner.

When assessing whether a penalty fee should be levied and the size of the penalty fee

special consideration must be given to the circumstances specified in ch. 6. § 4 BDL, i.e. if

the violation was intentional or due to negligence, the damage, danger or

violation that the violation entailed, the nature of the violation, degree of severity and

duration, what the personal data controller or personal data assistant did to

limit the effects of the breach, as well as if the personal data controller or

6 Cf. IMY's decision of 8 May 2013 (1552-2012).

7 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with

regarding the processing of personal data by competent authorities to prevent, prevent, investigate, disclose or

prosecute crimes or enforce criminal penalties, and the free flow of such data and on the suspension of

Council Framework Decision 2008/977/RIF.

the personal data assistant was previously ordered to pay a penalty fee. The enumeration is
not exhaustive but indicates the circumstances that are particularly important and there are
room to consider other aggravating or mitigating circumstances.

According to ch. 6 § 5 BDL, a penalty fee may be reduced in whole or in part if
the breach is excusable or it would be unreasonable to issue a penalty charge. The
the circumstance that a violation was due to the personal data controller not having
sufficiently good routines are not a reason to lower the penalty fee. 8

IMY notes that the Swedish Customs Service breached its responsibility for personal data when employees on
The authority has used Google Photos in customs crime operations. Regarding
the damage caused by the violations, there has been a lack of conditions to investigate
the people who appeared in pictures or in videos uploaded to Google Photos have
suffered any actual damage. It mainly has to do with the admissions that
stored in the cloud continuously deleted. For the same reason it has not been possible to
investigate in more detail which or how many appeared in the relevant images and
the movies. It is clear, however, that the Customs has lost control over an unknown number of different ones
categories of data that entailed a risk of harm. This applies regardless of the accounts
have been password protected.

According to IMY, there is reason to take a serious look at the risk of spread in situations such as
it is in question in this case. This is especially so when it comes to categories of
personal data that occur within law enforcement activities and that belong to them
nature are sensitive to privacy and need special protection. The lack of technical and
the organizational measures have resulted in the processing of personal data taking place
outside the control of the Swedish Customs Service with a private service provider and without anyone
preliminary assessment of the treatment's intrusion into the personal privacy of individuals. The

the fact that there was no opportunity to investigate the incident in more detail shows the importance of ensuring that information is processed within the own operational support so that the control of personal data or information covered by confidentiality does not be lost. The fact that there was a high probability of information about crimes or suspicion of crime or other data sensitive to privacy is to be regarded as one aggravating circumstance.9

IMY assesses that the circumstances explained above mean that it is a question if a serious violation partly justifies the levying of a penalty fee, partly that the fee is set at a relatively high amount.

However, a number of mitigating circumstances have also emerged in the case. It has to to begin with it was only a matter of a few employees who without the authority's approval used the current cloud service. Then the current employees discovered that material was stored in the cloud service, they have continuously deleted the images and movies uploaded, which reduced the risks of the treatment. Furthermore, have After the incident, the customs office took both technical and organizational measures measures to prevent similar incidents, including by clarifying guidelines and limit the possibilities of downloading applications. Even that one the fact that the incident came to IMY's attention through notification from The customs authority speaks in a mitigating direction.10 IMY notes, however, that in this case it is a question about an incident that the Customs Service according to ch. 3 Section 9 BDL is obliged to report to IMY. To the incident came to IMY's knowledge through the Customs Agency's notification can therefore only

8 Cf. prop. 2017/18:232 p. 485.

9 See prop. 2017/18:232 p. 484.

10 See prop. 2017/18:232 p. 331.

considered mitigating to a limited extent. The mitigating circumstances

are such that the penalty fee must be determined at a significantly lower amount than what

which was otherwise justified.

Based on an overall assessment, IMY decides that the Swedish Customs Service must pay a

penalty fee of SEK 300,000. Reasons that according to ch. 6 § 5 BDL fully or partially set

According to IMY, the penalty fee has not been reduced.

This decision has been taken by the general manager Lena Lindgren Schelin after a presentation

by the lawyer Jonas Agnvall. In the final proceedings, the Chief Justice David also has

Törngren and unit manager Charlotte Waller Dahlberg participated. It-

security specialist Johan Ma has participated in the assessments relating to

information security.

Lena Lindgren Schelin, 2022-03-14 (This is an electronic signature)

Appendix

How to pay penalty fee

Copy for information

The data protection representative: dataskyddsombud@tullverket.se

How to appeal

If you want to appeal the decision, you must write to the Swedish Privacy Protection Authority. Enter in

the letter which decision you are appealing and the change you are requesting. The appeal shall

have been received by the Privacy Protection Authority no later than three weeks from the date of the decision

was announced. If the appeal has been received in time, send

The Privacy Protection Authority forwards it to the Administrative Court in Stockholm

examination.

You can e-mail the appeal to the Privacy 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.