Decision

Diarienr

2020-12-10

DI-2019-9432

Umeå University

901 87 Umeå

Supervision according to the Data Protection Ordinance - Umeå

the university's processing of personal data

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 states that Umeå University

□

has sent sensitive and privacy-sensitive personal data through

unencrypted e-mail and via open network to the Police Authority on 5

February 2019. The university has therefore processed personal data in

contrary to Article 5 (1) (f) and Article 32 (1) and (2) (i)

the Data Protection Regulation1 by not having taken appropriate technical measures

measures to ensure an appropriate level of safety in

relation to the risk.

□

has not reported the personal data incident to the Data Inspectorate and

not documented the circumstances surrounding the incident then

the university became aware of it. The university has therefore

acted in breach of Article 33 (1) and (5) of the Data Protection Regulation.

□

in the processing of sensitive and privacy-sensitive personal data

in the cloud service Box, during the period May 25, 2018 to spring 2019, no

have taken appropriate technical and organizational measures to:

prevent unauthorized disclosure of or unauthorized access to

personal data. The university has therefore treated

personal data in breach of Article 5 (1) (f) and Article 32 (1) and (2) (i)

the Data Protection Regulation.

Administrative penalty fee

The Data Inspectorate decides on the basis of Articles 58 (2) and 83 i

the Data Protection Ordinance and Chapter 6 Section 2 of the Data Protection Act (2018: 218) to Umeå

the university must pay an administrative sanction fee of SEK 550,000.

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).

Report on the supervisory matter

Background

The Data Inspectorate began inspecting Umeå University on 29 August 2019.

The inspectorate had received information that the university had sent sensitive personal data to the Police Authority via unencrypted e-mail. To the information was attached to the Police Authority's letter; Information about shortcomings in handling documents.

The purpose of the supervision is to investigate whether the personal data processing as described in the Police Authority's letter meets the requirements for security as set out in Articles 5.1.f and 32 of the Data Protection Regulation.

The Data Inspectorate has also examined whether Umeå University has followed the provision of Article 33 of the Data Protection Regulation, as inter alia is about the personal data controller's obligation to report to a personal data incident.

Furthermore, the Data Inspectorate has investigated the handling of sensitive personal data in the cloud service Box made in accordance with data protection rules.

The Data Inspectorate's supervision will take effect from 25 May 2018 then the Data Protection Regulation came into force. The inspection therefore has not examined the incident that occurred before that date.

The supervision has been carried out through written communication.

What has emerged in the case

Letter from the police authority

The Police Authority's letter states, among other things, the following.

A research group at Umeå University requested all of them preliminary investigation report concerning rape against men in Sweden from 2014.

On 18 July 2016, the Police Authority released the documents by courier.

In connection with a request for supplementation via email attached

research group, 19 November 2017, unintentionally one of the

preliminary investigation report previously issued by the Police Authority. The police authority then contacted the research group and pointed out the inappropriateness of

to send sensitive material over unprotected email channels. The research group

regretted what had happened and referred to the human factor.

In connection with another request for supplementation attached

the research group, on 5 February 2019, again the same

preliminary investigation report. When the Police Authority contacted once again

the research group about this was admitted that this time too it was unintentional

attached the sensitive material in an email.

Information from Umeå University

Umeå University was responsible for personal data when the email was sent to

The police authority.

The principal researcher left his employment at Umeå University

on 31 August 2018 for employment at Uppsala University. Because it

the principal researcher changed employer and the workplace has the project

also changed residence. However, this happened after the current events.

The financier Forte2 decided to change the principal on 13 March 2019 and

The Ethics Review Authority approved the change, which involved a change

research principal at Uppsala University on 10 May 2019.

The research project at Umeå University has been approved by

The ethics review authority and the preliminary investigation protocols have been received

and stored on the basis of a public interest that allows

personal data processing.

The course of events

In August 2016, the research group received the preliminary investigation protocols that

requested. The documents were sent in paper form to Umeå University.

All police reports and preliminary investigation reports from 2014

scanned in and stored on a password-protected file surface. A physical version

locked in an archive room. The preliminary investigation protocols contain information

about, among other things, suspicion of crime, name, social security number and

contact information. In addition, these protocols contain information on

sexual life and health, ie sensitive personal data.

In a request for supplementation made in 2017, the intention was not to

attach the minutes among the other documents sent to

The police authority. After what happened, the research group has, among other things, introduced

a routine of scanning sensitive material separately.

The research group has not been able to explain why the group, on 5 February 2019,

once again attached the minutes in an email to the Police Authority.

Security when sending out the preliminary investigation protocols

The incorrect handling has been limited to two occasions. Otherwise have

project routines to lock in physical documents, to separate administrative

documents from research data and to password protect digital documents

followed. Only two researchers from the university have had access to the current

the material.

The university has, among other things, regulations and instructions to ensure

that the processing of personal data at universities complies with the requirements set out in

Article 32 of the Data Protection Regulation. The university has had a clear since 2014

rule that sensitive personal data may not be sent by e-mail, in accordance

with the document E-mail service at Umeå University. Employees get

continuous training and information on the subject. The university is also planning

to direct a special information effort on the processing of personal data in

e-mail to all employees at the university.

The university has made a mistake by sending sensitive

personal data via e-mail to the Police Authority.

The personal data processing in question can therefore not be said to meet those requirements

provided for appropriate security measures in accordance with Article 32 of

the Data Protection Regulation.

The personal data incident

Umeå University became aware that sensitive personal data had been sent

by e-mail in connection with the authority receiving the Data Inspectorate's

letter of supervision, 30 August 2019.

On September 2, 2019, the university conducted an analysis of the events and

then came to the conclusion that it was unlikely that the personal data incident would

may pose a risk to data subjects. The university has

documented the events in the Data Inspectorate's form for reporting

personal data incident. The university has stated in the form, among other things

following.

The university has decided that no report should be submitted to the Data Inspectorate. (…) The 2nd

September, a registered letter was received from the Swedish Data Inspectorate containing information about

the incidents. Umeå University's assessment is that it is unlikely that the incident resulted

high risk to individuals' freedoms and rights. There is no indication that anyone has occurred

actual damage or that any unauthorized person has accessed the information when the protocol in question has

sent to the authority that established it and to the administrator who had the task

to handle and provide the university with the same type of information.

Storage and access in the cloud service Box

The university has scanned in 108 preliminary examination protocols from 2014 as

saved locally on a personal computer and then uploaded to

cloud service provider Box.

The user can access the stored data in Box by logging in

via a web interface internally via the university's network with

single factor authentication (ie username and password).

It is also possible to log in externally via the internet on the university's website

umu.se. The login then takes place via any equipment / network. The user states

first their email address and then their college ID (username) and

password.

User accounts in Box are integrated and linked to university ID as in

in turn are integrated with SWAMID. With SWAMID, a safe is obtained

identification because passwords are neither saved nor sent to Box.

The authentication takes place before, by sending a "ticket" to Box som

confirms the authorization.

All communication is encrypted with 256 bit SSL encryption (https).

All information is stored with 256-bit encryption. This means that

the information is not available if someone without authorization would have access

to it. Backups are also encrypted. Box stores the encryption keys separately

from data.

The research project includes two researchers and only the two have had

access to and access to the file area provided by Box. Since

access has been restricted, no special procedures have been established.

The university has a personal data assistant agreement with SUNET (Swedish

University computer Network) which, among other things, applies to storage of

preliminary investigation protocols. SUNET has in turn hired the Deputy Assistant Box.

Box stores the information in the United States and is connected to the Privacy Shield and has

signed binding corporate regulations.

The preliminary investigation protocols are covered by secrecy in accordance with ch. § 1 and 11

Cape. Section 3 of the Public Access to Information and Secrecy Act (2009: 400), OSL. Starting point

is thus that confidentiality applies to the information.

Information that sensitive personal data should not be stored in Box has

published on the university's intranet in September 2016.

The university has made the assessment that there are legal and

safety conditions for storing both sensitive and

confidential information in Box. However, the university has in connection with its

risk and vulnerability analysis for precautionary reasons judged that this should not happen.

The university has assessed that the file surface maintains a satisfactory level of safety.

The assessment has been based on security measures such as access, access and

authorization and security in communication.

Justification of decision

Applicable rules

The responsibility of the personal data controller

The Data Protection Regulation is the primary legal regulation in processing

of personal data.

The person responsible for personal data is responsible for being able to show that they

the basic principles of Article 5 of the Data Protection Regulation are complied with (Article

5.2).

The person responsible for personal data is responsible for implementing appropriate technical information

and organizational measures to ensure and be able to demonstrate that

the processing is performed in accordance with the Data Protection Regulation. The measures shall

carried out taking into account the nature, scope, context of the treatment

and purposes and the risks, of varying degrees of probability and severity, for

freedoms and rights of natural persons. The measures must be reviewed and updated

if necessary. This is stated in Article 24 (1) of the Data Protection Regulation.

Legal basis

Article 6 of the Data Protection Regulation states the following.

A treatment is only legal if one of the conditions specified in the article is

met (paragraph 1).

A processing is legal if it is necessary to perform a task of

public interest (paragraph 1 (e)). Research purposes are considered a task of

public interest.

The task of general interest must be established in accordance with Union law

or national law (paragraph 3). For state universities and colleges are

the research task established in ch. the Higher Education Act (1992: 1434).

As a general rule, it is forbidden to process sensitive personal data

for example, personal data on health and sexual life. However, there are a number

derogation from the prohibition in Article 9 (2) of the Data Protection Regulation. Of Article 9 (2) j

in the Data Protection Regulation it follows that the processing must be necessary for

research purposes and shall be subject to appropriate safeguard measures for it

rights and freedoms of data subjects in accordance with Article 89 (1) (i)

the Data Protection Regulation.

In addition, the exemption from this prohibition requires that national law contain

provisions on appropriate and specific measures to ensure it

registered privacy. One is established in the Ethics Review Act3

3

The Act (2003: 460) on ethical review.

appropriate and specific action required in the treatment of sensitive

personal data for research purposes. Also provisions on secrecy in

OSL is an example of such an appropriate and special measure.

Article 89 (1) of the Data Protection Regulation sets out specific conditions for processing

of personal data for research purposes. It states that

the treatment shall be subject to appropriate protective measures in accordance with

Regulation.

The requirement for security in the processing of personal data

A basic principle for the processing of personal data is the requirement

security in accordance with Article 5 (1) (f) of the Data Protection Regulation, which states that:

personal data shall be processed in a manner that ensures appropriate

security of personal data, including protection against unauthorized or unauthorized use

treatment and against loss, destruction or damage by accident,

using appropriate technical or organizational measures.

It follows from Article 32 (1) of the Data Protection Regulation that

the person responsible for personal data and the personal data assistant shall take appropriate steps

technical and organizational measures to ensure a level of security

which is appropriate in relation to the risk of the treatment. That too

taking into account recent developments, implementation costs and

the nature, scope, context and purpose of the treatment and the risks, of

varying degrees of probability and severity, for the rights of natural persons and

freedoms.

When assessing the appropriate level of safety, special consideration shall be given to them

risks posed by the treatment, in particular from unintentional or illegal

destruction, loss or alteration or to unauthorized disclosure of or unauthorized

access to the personal data transferred, stored or otherwise

treated. This is stated in Article 32 (2) of the Data Protection Regulation.

Recital 75 of the Data Protection Regulation states that various factors must be taken into account in

the assessment of the risk to the rights and freedoms of natural persons. Among

otherwise, personal data covered by the duty of confidentiality, data on

health or sexual life. Furthermore, consideration must be given to whether the treatment applies

personal data about vulnerable natural persons, in particular children, or about

the processing involves a large number of personal data and applies to a large

number of registered.

Recitals 39 and 83 also provide guidance on the more detailed meaning of

the requirements of the Data Protection Regulation for security in the processing of

personal data.

If the personal data controller hires a personal data assistant to

carry out a processing, the data controller shall only use

personal data assistants who provide sufficient guarantees to implement

appropriate technical and organizational measures. It should be done in such a way

that the processing meets the requirements of the Data Protection Regulation and that it

data subjects' rights are protected. It is clear from Article 28 (1) and recital 81 in the preamble

the Data Protection Regulation. These provisions also state how the relationship

between the personal data controller and the personal data assistant shall be regulated.

Obligation to report and document personal data incidents

According to Article 4 (12) of the Data Protection Regulation, a personal data incident is a

safety incident leading to accidental or unlawful destruction, loss or

change or to unauthorized disclosure of or unauthorized access to the

personal data transferred, stored or otherwise processed. According to

Article 29 Group Guidance WP2504 may be unauthorized or illegal

processing include the disclosure of personal data (or access to

these) to recipients who are not authorized to receive (or access)

the data, or any other form of processing that is contrary to

the Data Protection Regulation.

Article 33 (1) of the Data Protection Regulation states that

the person responsible for personal data, in the event of a personal data incident, must report

the incident to the supervisory authority without undue delay, and if so

possible not later than 72 hours after learning of it. If it is

it is unlikely that the personal data incident entails a risk to natural persons

rights and freedoms need not be notified. About one

the person responsible for personal data does not act quickly and it becomes obvious that one

Article 29 - Working Party on Data Protection, WP250rev.01; Guidelines for notification of

personal data incidents according to Regulation (EU) 2016/679; adopted on 3 October 2017; last

reviewed and adopted on February 6, 2018; adopted by the European Data Protection Board, EDPB,

during the first plenary session on 25 May 2018; pp. 11–12. The working group was set up

pursuant to Article 29 of Directive 95/46 / EC and was an independent EU advisory body in matters

concerning data protection and privacy.

incident has taken place, this can be considered as a failure to act in

in accordance with Article 335.

The following is stated in recital 85.

A personal data incident that is not quickly remedied appropriately can for natural persons

lead to physical, material or intangible damage, such as loss of control over one's own

personal data or to limit their rights, discrimination, identity theft

or fraud, financial loss, unauthorized revocation of pseudonym, damage to reputation,

loss of confidentiality in respect of personal data covered by the obligation of professional secrecy, or

to another economic or social detriment to the natural person concerned. As soon as one

personal data controller becomes aware that a personal data incident has occurred, it should

personal data controllers therefore report the personal data incident to the supervisory authority

without undue delay and, if possible, within 72 hours of becoming aware of

this, unless the person responsible for personal data, in accordance with the principle of responsibility, can demonstrate that

it is unlikely that the personal data incident will entail a risk of physical

rights and freedoms of persons.

According to the Article 29 Working Party, a data controller shall be deemed to have received

knowledge of the incident when the data controller is reasonably certain

that a security incident has taken place which has resulted in personal data

endangered. The data controller shall, in accordance with the Data Protection Regulation,

take all appropriate technical protective measures and all appropriate organizational

measures to immediately determine whether a personal data incident has taken place

room and promptly inform the supervisory authority and the data subjects.

Recital 87 of the Data Protection Regulation states the importance of being able to establish one

incident, assess the risk to individuals and then report the incident if so

required.

Article 33 (5) of the Data Protection Regulation regulates the obligation to:

document personal data incidents. The person responsible for personal data shall

document all personal data incidents, regardless of whether the incident should

reported to the Data Inspectorate or not. The documentation must contain

information about the circumstances surrounding the personal data incident, its

effects and the corrective measures taken. The documentation must

enable the supervisory authority to monitor compliance with

Article 33 of the Data Protection Regulation.

5

WP250, rev01, p. 13.

The documentation obligation in Article 33 (5) is also linked to

liability in Article 5 (2) of the Data Protection Regulation, ie

the person responsible for personal data must be responsible for and be able to show that they

the basic principles of data protection are complied with. There is also one

link between Article 33 (5) and the provision on liability for

data controller in accordance with Article 24 of the Data Protection Regulation.6

It may be added that the Article 29 Working Party's guidelines state that it

personal data controllers need to have routines to detect and remedy

incidents involving personal data, which is the meaning of Article 33 (5).

In addition, it shows the ability to quickly detect, remedy and report

an incident should be seen as important elements in the appropriate technical and

organizational measures referred to in Article 32 of the Data Protection Regulation.

Transfer of personal data to third countries

Chapter V of the Data Protection Regulation sets out the possibilities for:

transfer personal data to a third country (a country outside the EEA).

Personal data may be transferred if the European Commission has decided to do so

there is an adequate level of protection in the recipient country or if there is one

appropriate safeguards, for example through contractual clauses or binding

company regulations.7

For recitals 101 and 116 of the Data Protection Regulation, the risk is emphasized when

personal data are transferred to countries outside the Union and the importance of:

the level of protection will not be lower in such transfers. This is especially true in

question of the protection against unauthorized use or unauthorized disclosure of

this information. Furthermore, the person responsible for personal data and

the personal data assistant's responsibility to ensure that the regulation is complied with.

The Data Inspectorate's assessment

Personal data responsibility

The Data Inspectorate states that Umeå University is

personal data controller for the processing of personal data that

6

7

WP250, rev01, p. 28.

See Articles 44 to 50 of the Data Protection Regulation.

updated in the case until the project was transferred to Uppsala

university in the spring of 2019.

Processing of personal data in unencrypted e-mail and open network

The Data Inspectorate states that Umeå University, within the framework of

research project, has sent a preliminary investigation report concerning

rapes of men in an unencrypted e-mail via an open network to

The police authority. Something that the university has also admitted.

The preliminary examination report contains information on health and sexual life which are sensitive personal data. Processing of sensitive personal data can involve significant risks to personal integrity and are therefore required strong protection in the processing of such data.

The preliminary investigation report also contains information on suspicion about crimes and social security numbers that are so-called privacy-sensitive personal data. The processing of this type of personal data is therefore off such that the data must have strong protection. That means if about these personal data sent by e-mail, they must be protected in such a way that unauthorized persons cannot take part in them. Personal data can, for example protected by encryption.

Sending information with unencrypted e-mail means that other than that the intended recipient can access the information in the e-mail. Thus it is not ensured that only the intended recipient takes part personal data.

The university has also sent the personal data via an open network. One open network, such as the internet, is characterized by others being able to take part in it information communicated on the network. This means that unauthorized persons have been able to gain access to the personal data transferred by the university.

As the person responsible for personal data, Umeå University must ensure that the technical and the organizational measures ensure a level of security that is appropriate in in relation to the risks to the rights and freedoms of natural persons which the treatment entails (Article 32 (1)). The personal data that is processed must for example, protected against unauthorized disclosure or unauthorized access.

What is the appropriate level of safety varies according to the risks, the nature, scope, context and purpose of the treatment. At

the assessment must therefore, for example, take into account what type it is

personal data processed.8

The university must identify the possible risks for those registered

rights and freedoms and assess the likelihood of risks occurring

and the consequences in such cases.

In this case, it is a question of both sensitive and privacy-sensitive ones

personal data. Processing this type of data requires a strong

protection based on the nature of the treatment.

Overall, the Data Inspectorate finds that Umeå University has processed

personal data in violation of the Data Protection Ordinance by the University

have not taken appropriate technical safety measures to protect

the personal data in the e-mail based on the sensitivity of the data and

how they were communicated unencrypted over open network. The treatment has therefore

in breach of Article 5 (1) (f) and Article 32 (1) and (2) (i)

the Data Protection Regulation.

The personal data incident should have been documented and reported

According to Umeå University, the university became aware of being sensitive

personal data sent via unencrypted e-mail by the university

received the Data Inspectorate's supervisory letter on 30 August 2019. According to

the university also documented the incident, on September 2, 2019, in

The Data Inspectorate's form for reporting personal data incidents.

As regards the knowledge of the incident, the Data Inspectorate states that it is off

The police authority's letter dated 3 April 2019, states that

The police authority in contact with the university pointed out the inappropriateness of that

send sensitive personal information via unencrypted e-mail. The Data Inspectorate

therefore considers that the university must have become aware of the current situation

the incident before 30 August 2019 and at least no later than 3 April 2019.

With regard to the documentation, the Data Inspectorate thus finds that

the university did not document the circumstances surrounding

the personal data incident immediately after becoming aware of it. This

makes it difficult to monitor compliance with Article 33 of the

8

See recitals 75 and 76 of the Data Protection Regulation.

the Data Protection Regulation. That the university has subsequently filled in

The Data Inspectorate's form for reporting personal data incidents changes

not the assessment that the university should have documented the incident already

when the Police Authority contacted the university.

Furthermore, the Swedish Data Inspectorate states that the university has not been admitted

with a report of a personal data incident to the Data Inspectorate. According to

the university was due to the fact that it was unlikely that the incident would

entail a high risk for individuals' freedoms and rights. The Data Inspectorate wants

emphasize that there is always a risk that unauthorized persons may take part in it

the personal data if it is sent unencrypted via the open network. As

The Data Inspectorate previously stated that the mailing applies to both sensitive and

privacy-sensitive personal data. The risk for the data subjects' freedom and

rights are therefore high if this type of personal data is processed in one

in such a way that they, for example, benefit from unauthorized persons.

All in all, the Data Inspectorate finds that Umeå University has failed

to act in accordance with Article 33 (1) and (5) of the Data Protection Regulation.

Storage of sensitive personal data in a cloud service in third countries

Umeå University has used the cloud service Box to store 108

preliminary investigation report on rape of men.

A cloud service is an Internet-based IT service provided by an external party

supplier. The service can include storage but also other functions, there

these are wholly or to some extent outside the internal operations of the company

it environment9. In this case, the storage is outside the university's internal IT environment. Via the personal data assistant

SUNET, Umeå University is hired

Deputy Assistant Box.

The Data Protection Regulation does not only require that it

the person responsible for personal data shall ensure appropriate security for

personal data. The regulation also requires that it

the person responsible for personal data ensures that the personal data assistant fulfills one

security level when processing personal data for it

on behalf of the data controller.

For further definitions see Article 29 Data Protection Working Party, 01037/12 / EN WP

196, Opinion 05/2012 on Cloud Computing.

9

The person responsible for personal data is also responsible for ensuring that the person who
the personal data assistant in turn hires meets the requirements in
the Data Protection Regulation.

Box is supplied by a US company that stores the information in the US.
According to the university, Box was connected to the Privacy Shield and had signed
binding corporate rules.

Personal data may be transferred to third countries only if the conditions in Chapter V of
the Data Protection Regulation are complied with. This applies provided that it
the personal data controller and the personal data assistant can ensure that it
the level of protection afforded to natural persons by the Regulation is not undermined.

According to a decision by the European Commission10, it has been allowed for
personal data controllers in the EU to transfer personal data to recipients who
has joined the Privacy Shield.

In the so-called Schrems II case11 of 16 July 2020, however
The European Court of Justice that the Privacy Shield agreement between the EU and the US does not provide
adequate protection of personal data when it is transferred to the United States. The
means that EU data controllers are no longer allowed to:
with the support of Privacy Shield transfer personal data to the United States.

The Schrems II target may also affect transfers of
personal data that takes place with the help of binding company regulations. The
as the legislation of a third country may affect the protection afforded
through these provisions. The European Court of Justice has ruled that it is
personal data controller who must assess the level of protection required according to
EU law is complied with in the third country concerned.

The Data Inspectorate states that Umeå University ceased to process

the current personal data in the cloud service Box in the spring of 2019. Then it was

allowed by the European Commission decision to transfer personal data to the United States

with the support of Privacy Shield. The Data Inspectorate therefore stays current

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to

Directive 95/46 / EC of the European Parliament and of the Council on whether adequate protection is ensured

through the shield of privacy in the EU and the United States.

11 Case C-311/18 - Data Protection Commissioner v Facebook Ireland and Maximillian

Scares.

case stating that Box is said to have been connected to the Privacy Shield

at that time and that the treatment at the university had ended before

The Schrems II goal.

In addition to the person responsible for personal data having support to transfer

personal data to third countries, the person responsible for personal data is also responsible

for the personal data assistant to process the data in a way that

ensures adequate security.

That personal data, like the personal data assistant, is located in a third country

may increase the risk that natural persons will not be able to exercise their

data protection rights, in particular to protect against unauthorized access

use or unauthorized disclosure of this information.12

In this case, it is a matter of information that is protected by confidentiality.

In order to be allowed to process sensitive personal data, the Data Protection Ordinance sets

requirement that national law contain provisions on appropriate

and special measures. The provisions on secrecy to protect it

individuals is such regulation that protects the integrity of individuals in handling

of public documents.13 This means that secrecy is one

privacy protection measure such as the personal data controller and

the personal data assistant has to follow. When the personal data is stored with a

actor who is not covered by secrecy, this means weaker privacy protection

for the data, as a statutory duty of confidentiality that is

punitive sanctions provide stronger protection than an agreed duty of confidentiality.14

Since Box is an actor that is not covered by OSL, the personal data is given one

weaker privacy protection.

There are also technical weaknesses in the selected storage.

To gain access to the preliminary examination protocols in Box, the university has

used a so-called single factor authentication. In this case, college ID

(username and password.

12

13

14

Cf. recitals 101 and 116 of the Data Protection Ordinance.

See the bill New Data Protection Act (Bill 2017/18: 105 p. 116).

JO's decision of 9 September 2014, no. 3032-2011.

The authentication is used so that the person responsible for personal data can see

that only authorized users have access to personal data.

Single-factor authentication is a weak form of authentication. The risk of someone

can get access to username and password is great. Besides, it is not

surely the one who has been robbed will discover that this has happened

if someone comes across username and password through for example so

called phishing.

Stronger authentication should make it harder for unauthorized people to get over them

necessary login information needed to be able to authenticate.

Stronger authentication can be achieved by using more than one

factor (something you know, something you have and something you are). For example, can

"Something you know" can be a username or password, "something you have" can

be a smart card or mobile phone and "something you are" can be one

fingerprints or facial features.

The user can access the stored data in Box by logging in

via a web interface internally via the university's network with

single factor authentication (ie username and password). The

can also log in externally via the internet on the university's website umu.se.

The login then takes place via optional equipment and optional network and the user

first states his e-mail address and then his college ID (username)

and password (that is, with single-factor authentication).

Because access to the current data can be via the open network is

the exposure area to unauthorized persons is very large, which entails the risk of

the data will unauthorized to part increases.

Umeå University has stated that the communication and storage of

the information in the preliminary investigation protocols has been encrypted in Box.

However, the Data Inspectorate does not consider that this means that the information is

adequately protected against unauthorized access. For example, it may be illegal
come across usernames and passwords pretending to be authorized and thus
take part of the information in clear text.
As previously stated, the person responsible for personal data must ensure a suitable one
safety in relation to the risk of treatment. This also applies when

the personal data is processed by a personal data assistant. The
personal data controllers must therefore make an assessment of the risks that
may occur during treatment. When the personal data controller
processes personal data in a cloud service, the person in charge needs to implement
a suitability assessment that includes a risk analysis. That way, it gets
personal data controller a basis for being able to make decisions about which
appropriate technical and organizational measures that are needed or should be
required by the personal data assistant. It also provides the person responsible for personal data
an opportunity to ensure an appropriate level of security.
When assessing the security level when storing and transferring
personal data shall be given special consideration if the processing entails a risk of
unauthorized disclosure or unauthorized access.
Umeå University has stated that the university in connection with its risk and
vulnerability analysis judged that sensitive personal data should not be stored in Box
for precautionary reasons. This information was published at the university
intranet in September 2016. Despite the university scanned in
pre-investigation protocols and stored them in Box.

The preliminary investigation protocols concern rapes against men and personal data in them are both sensitive and privacy-sensitive. The information is covered in addition to secrecy. The Data Inspectorate's assessment is that the processing of this type of personal data involves a high risk to the privacy of individuals if the personal data is disclosed or if an unauthorized person gains access to it. The treatment is therefore of such a nature that it requires a high level of safety.

The Data Inspectorate states that it has been a question of a treatment of personal data in a cloud service in the United States that is not covered by the regulations in OSL, and that security has not been high enough to prevent unauthorized access to the data. In addition, the Data Inspectorate states that the university in 2016 assessed that the processing of sensitive personal data in Box was not appropriate.

In summary, the Data Inspectorate finds that Umeå University does not have have taken appropriate technical and organizational measures to prevent unauthorized disclosure of or unauthorized access to the sensitive and privacy-sensitive personal data stored in Box. The university has thereby not ensuring a level of safety that is appropriate in relation to

the risk of processing the personal data in question in the case.

Umeå University has thus processed the personal data in violation of Article 5 (1) (f) and Article 32 (1) and (2) of the Data Protection Regulation.

Choice of intervention

Legal regulation

In the event of violations of the Data Protection Ordinance, the Data Inspectorate has a number corrective powers, including reprimand, injunction and penalty fees. It follows from Article 58 (2) (a) to (j) of the Data Protection Regulation.

The Data Inspectorate shall impose penalty fees in addition to or instead of other corrective measures referred to in Article 58 (2), the circumstances of each individual case.

Member States may lay down rules on whether and to what extent administrative penalty fees may be imposed on public authorities. This is stated in Article 83 (7) of the Regulation. Sweden has accordingly decided that the Data Inspectorate shall be allowed to charge sanction fees by authorities.

For violations of, among other things, Articles 32 and 33, the fee shall amount to a maximum of SEK 5,000,000. For infringements of, inter alia, Article 5 i According to the ordinance, the fee shall amount to a maximum of SEK 10,000,000. It appears from Chapter 6 Section 2 of the Data Protection Act and Article 83 (4) and (5) i the Data Protection Regulation.

If a personal data controller or a personal data assistant, with respect to on one or the same or interconnected data processing, intentionally or through negligence violates several of the provisions of this Regulation the total amount of the administrative penalty fee may not exceed it amount determined for the most serious infringement. It appears from Article 83 (3) of the Data Protection Regulation.

Each supervisory authority shall ensure that the imposition of administrative penalty fees in each individual case are effective, proportionate and deterrent. This is stated in Article 83 (1) of the Data Protection Regulation.

Article 83 (2) sets out the factors to be taken into account in determining whether a administrative penalty fee shall be imposed, but also what shall affect

the size of the penalty fee.

The size of the penalty fee

The university has sent a preliminary investigation protocol with personal data

about, among other things, health, sexual life and suspicion of crime via unencrypted email and through open network. The

personal data processed is both

sensitive and privacy sensitive and covered by regulations on

secrecy.

The police authority sent the information to the university via courier, which should

made the university aware of the data value of the data. Despite this

failed the university to take appropriate technical safety measures.

The personal data was thus not protected from the risk of being exposed to, among other things

other unauthorized disclosure and unauthorized access. The Data Inspectorate finds that

no other assessment can be made than that the infringement took place through

negligence.

In addition, Umeå University has stored a large number, 108 pieces,

preliminary investigation protocols with sensitive and privacy sensitive

personal data in the cloud service Box. This without the university ensuring

an appropriate level of security to be able to store this type of personal data in

Box. The university thus also failed in this part to take appropriate

technical safety measures. The university also did not ensure that

personal data were covered by such appropriate organizational measures

required by the data protection regulations.

Contrary to its own risk and vulnerability analysis, the university stored them
sensitive personal data in Box. The Data Inspectorate considers this to be one
factor that must be taken into account when assessing the size of the penalty fee.
Furthermore, the university has failed to report the personal data incident as
occurred at the time of sending the e-mail to the Data Inspectorate. Nor
the circumstances surrounding the incident were documented when the university became
paid attention to it.
Against this background, the Data Inspectorate finds that Umeå University through
the personal data processing in question has violated Article 5 (1) (f), Article
32 (1) and (2) and Article 33 (1) and (5) of the Data Protection Regulation.
The Data Inspectorate therefore considers that Umeå University should be applied
administrative penalty fees for the said infringements.

The Data Inspectorate finds that the treatments via e-mail and storage in
Box refers to two interconnected data processing operations in accordance with Article 83 (3) (i)
the Data Protection Regulation. This is because the treatments are the same
personal data within a research project and refers to violation of the same
provisions, ie Article 5 (1) (f) and 32 (1) and (2) of the Regulation.
When determining the size of the penalty fee, the Data Inspectorate takes into account
the above circumstances and that the administrative penalty fee
shall be effective, proportionate and dissuasive. That Umeå University does not
has met the security requirements is serious when it comes to personal data
of such a type that the data require strong protection based on the processing

species.

The Data Inspectorate decides on the basis of an overall assessment that Umeå

universities must pay an administrative sanction fee of a total of 550,000

kronor. For the mailing in the e-mail and the storage in the cloud service Box

the university must pay a fee of SEK 450,000. For the university

failure to report the personal data incident to the Data Inspectorate

and for not having documented the incident, the university must pay a fee

of SEK 100,000.

This decision was made by the Director General Lena Lindgren Schelin after

presentation by lawyer Linda Hamidi. In handling the case has

lawyer Caroline Cruz Julander participated. At the final processing

The unit managers Katarina Tullstedt and Malin Blixt and the IT security specialists Johan Ma and Ulrika Sundling have

participated.

Lena Lindgren Schelin, 2020-12-10 (This is an electronic signature)

Appendix

Information on payment of penalty fee.

Copy for information to

The Data Protection Officer.

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.