Decision

Diary no

2020-12-02

DI-2019-3842

Aleris Närsjukvård AB

Box 6401

113 82 Stockholm

Stockholm County

Supervision according to the data protection regulation and

patient data act- needs and risk analysis and

questions about access in records systems

Table of Contents

The Swedish Data Protection Authority's decision

In the review on April 24, 2019, the Norwegian Data Protection Authority found that

Aleris Närsjukvård AB (formerly Praktikertjänst N.Ä.R.A. AB) treats

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

personal data in violation of article 5.1 f and 5.2 as well as article 32.1 0ch 32.2 i

the data protection regulation1 by

1.

Aleris Närsjukvård AB has not carried out a needs and risk analysis

before authorizations are assigned in the TakeCare records system

and National patient overview (NPÖ) in accordance with ch. 4. § 2 and

6 ch. Section 7 of the Patient Data Act (2008:355) and Chapter 4. § 2 of the National Board of Health and Welfare

regulations and general advice (HSLF-FS 2016:40) on record keeping

and processing of personal data in healthcare. This

means that Aleris Närsjukvård AB has not taken the appropriate measures

organizational measures to be able to ensure and be able to demonstrate that

the processing of the personal data has a security that is suitable in

relation to the risks.

2. Aleris Närsjukvård AB does not limit users' authorizations for

access to the record system TakeCare and NPÖ to what only

is needed for the user to be able to fulfill his tasks

within health care in accordance with ch. 4 § 2 and ch. 6 Section 7

the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40. This means that

Aleris Närsjukvård AB has not taken measures to be able to

ensure and be able to demonstrate appropriate security for the personal data.

Datainspektionen decides with the support of articles 58.2 and 83 i

data protection regulation that Aleris Närsjukvård AB for the violations

of Article 5.1 f and 5.2 and Article 32.1 and 32.2 i

data protection regulation must pay an administrative penalty fee of

12,000,000 (twelve million) kroner.

Datainspektionen orders with the support of article 58.2 d i

the data protection regulation Aleris Närsjukvård AB to implement and

document the required needs and risk analysis for the record systems

TakeCare and NPÖ and that subsequently, with the support of the needs and risk analysis,

assign each user individual authorization for access to

personal data that is limited to only what is necessary for it

individuals must be able to fulfill their duties within health and medical care,

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

natural persons with regard to the processing of personal data and on the free flow of

such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation).

in accordance with article 5.1 f and article 32.1 and 32.2 of the data protection regulation,

4 ch. § 2 and ch. 6 Section 7 of the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40.

Account of the supervisory matter

The Swedish Data Protection Authority initiated supervision by means of a letter on 22 March 2019 and has on site on April 24, 2019 reviewed Aleris Närsjukvård AB's decision on assignment of authorizations has been preceded by a needs and risk analysis.

The review has also included how Aleris Närsjukvård AB allocated authorizations for access to the main record system TakeCare and NPÖ, and which access possibilities the assigned permissions provide within the framework as well for the internal secrecy according to ch. 4. the Patient Data Act, as it coherent record keeping according to ch. 6 the patient data act. Beyond this the Data Inspectorate has also reviewed the documentation of access (logs) found in the journal systems.

The Swedish Data Protection Authority has only reviewed users' access options the journal systems, i.e. which care documentation the user can actually take part of and read. The supervision does not include which functions are included in the authorization, i.e. what the user can actually do in the records systems (eg issuing prescriptions, writing referrals, etc.).

The inspection is one of several inspections within the framework of a self-initiated one supervisory project at the Data Inspectorate, where i.a. Karolinska The University Hospital has been included. Due to what has emerged about Aleris Närsjukvård AB's view of the technical possibilities to limit the read access of its users in TakeCare, Aleris was asked Närsjukvård AB to specifically comment on a statement from Karolinska University Hospital, which also uses TakeCare, where the technical the possibilities regarding TakeCare were described.

What emerged in the case

Aleris Närsjukvård AB has essentially stated the following.

Personal data responsibility

Aleris Närsjukvård AB is the personal data controller and care provider.

The business

On 15 May 2019, Praktikertjänst N.Ä.R.A. AB with a letter to

The Swedish Data Protection Authority with information that Praktikertjänst N.Ä.R.A. AB

divested from the Praktikertjänst group (org. no. 556077-2419) on April 1

2020 and changed name to Aleris Närsjukvård AB (org. no. 556743-1951). With

because of this, the Swedish Data Protection Authority requested supplementary information

from Aleris Närsjukvård AB. Among other things, it appears from the additions

following.

On October 1, 2019, Aleris Healthcare AB (reg. no. 556598-6782) is purchased with

subsidiary up of Triton. In connection with the acquisition, the new is created

the group parent company, Aleris Group AB (reg. no. 559210-7550).

On April 1, 2020, Proliva AB (reg. no. 556472-1958) and associated

subsidiary up of Triton. Proliva AB acquires Aleris Group AB as

group parent.

Internship N.Ä.R.A. AB was owned before April 1, 2020, to one hundred

percent of Provliva AB. Provliva AB was in turn wholly owned by

group parent company Praktikertjänst AB.

After the divestment on April 1, 2020, Aleris Närsjukvård AB continues to be owned as one

one hundred percent of Proliva AB and is thus part of Aleris Group AB.

Proliva AB is in turn wholly owned by Aleris Healthcare AB.

The group parent company for the entire "Aleris Group" including the "Proliva Group" is Aleris Holding AB (reg. no. 559210-7535).

The following picture shows the ownership structure of Aleris Närsjukvård AB after the divestment on April 1, 2020.

Group turnover for Aleris Group AB amounted to SEK 1,215,385,000 between October 1, 2019 and December 31, 2019. Because Aleris Group AB was formed in connection with the change of ownership when Aleris Healthcare AB with subsidiaries were acquired, only turnover figures are available for this period.

The annual turnover for Aleris Healthcare AB amounted to SEK 30,223,866 during 2019.

Journal system

Aleris Närsjukvård AB uses TakeCare as the main record system within the framework of the internal confidentiality and participates in TakeCare's system for coherent record keeping. TakeCare has been used by Aleris Närsjukvård AB since 2009. Digital medical records were still a relative novelty in 2009 and these were primarily focused on patient safety by the documentation was designed based on medical-nursing needs as well as introduction of medication records. Aleris Närsjukvård AB has over the years at follow-up meetings with CompuGroup Medical (CGM), which is a supplier of

the journal system and is responsible for the functions that the system has to control

authorizations, and Center for Collaboration TakeCare (CSTC), pointed out shortcomings concerning patient safety and data security.

Aleris Närsjukvård AB also uses the National Patient Overview, NPÖ, within the framework for the coherent record keeping.

The number of patients and employees

The number of registered patients in TakeCare, at Aleris Närsjukvård AB, amounted to 55,061 at the time of the inspection.

The number of employees at Aleris Närsjukvård AB was at the time of the inspection to 1,150 monthly employees. The number of executives who have access to TakeCare amounted to 1,700, which essentially also includes ST doctors, contracted staff and students. The number 1,700 corresponds active accounts. The difference between active accounts and employees is because there is a lot of hired staff and at the time of inspection there was one hundreds of students who practiced at Aleris Närsjukvård AB.

The number of employees who have access to NPÖ amounted to the inspection time to 335 and consists mostly of doctors (158 doctors, 87 nurses, 82 physiotherapists, 4 occupational therapists, 3 medical secretary and 1 chiropractor).

Internal confidentiality

Needs and risk analysis

Aleris Närsjukvård AB has essentially stated the following.

There is a template for needs and risk analysis, Assignment of permissions,

needs and risk analysis, template: Job descriptions and assignments, and it is

business managers and unit managers who must carry out needs and

the risk analysis before assigning authorizations in the systems.

The template shows, among other things, that risks and needs must be weighed before the allocation of

an authorization profile and that it is the responsible manager who carries out a needs and

risk analysis of the employee's need for permissions to access by

personal data. The assessment is made, among other things, based on work tasks and

workplace. If the employee needs access to TakeCare for

the purpose "Reading and writing in a care relationship" this box is ticked by the manager.

Furthermore, three questions must be answered by the responsible manager by ticking one

or two boxes with statements under each question. One of these three questions concerns

patient integrity - "What risks regarding patient integrity does it mean that

permission granted? (justify in terms of access to patient data)'. The

there are two statements that can be ticked:

- "Opportunity to actively choose to open another journal within

the blocking area (care area) through its authority (remove internal

privacy)", or

- "Risk of access to, for the occasion of care, unnecessary patient information

in TakeCare through the possibility of cohesion

journal/read permission”.

It also appears that if the responsible manager answers no to any of the statements
the need for authorization must be considered once more before authorization is granted and
justification must be stated in writing.

There is a routine associated with the template, Assessment of Permissions for
access to data on patients as well as to other systems, and that routine
is stated to constitute instructions to the operations manager and unit manager how he
shall proceed when assigning authorizations. The routine shows that
authorizations to electronic systems containing patient data shall
is limited to what is needed for the employee to be able to fulfill their duties
tasks in healthcare. Furthermore, it appears that the manager, in connection with a new
employees' access to employment, make an assessment of which
permissions the new employee needs. There are no additional ones
instructions, but instead refer to another document.

When ordering permissions, the support function can provide feedback
if they see something that is perceived as very deviant. That the practical
the work with setting up authorizations in TakeCare is separated from
the managers, therefore becomes a control function in relation to the managers.

There is no "ready-made answer template" for what a risk analysis should look like, but
the risk analysis consists of the current business manager or head of unit doing one
assessment which it can then record in a free text box in the document
Assignment of authorizations – needs and risk analysis, template:
Functional descriptions and assignments.

The business manager or unit manager must answer the question in the template that reads:

"Which risks would an overly limited authorization assignment entail?"

Examples of responsible manager's risk analyzes regarding whether employees have

need for access to information in TakeCare is:

□

"No need based on patient safety that the employee has

authorization in TC or other patient-related systems".

□

"Reduced availability for patients as collaboration takes place with both

geriatrics such as ASIH and SPSV to optimally use personnel

resources. Reduced continuity for patients or risk of

Patient-safe record keeping of drug administration."

□

"Make patient work more difficult and prevent the possibility of helping each other

to maintain availability for patients at work peaks or

absence. Also hinder the possibility of frequent extra sessions in others

ASIH Team".

Authorization assignment for access to personal data

Aleris Närsjukvård AB has essentially stated the following.

Aleris Närsjukvård AB uses products produced by the company Acceptus

authorization templates in TakeCare. Acceptus is a central manager of TakeCare.

Based on which authorizations are included in these templates

Aleris Närsjukvård AB made its own list of different authorizations and needs

as the roles have.

The assignment of authorization is generally done in the following way. In a first layer

is there a "basis" for the allocation, e.g. the role of nurse or doctor. IN
the second layer is assigned permissions based on which device the user is working on
on, e.g. "Handen-geriatrics" and in the third layer authorization is added from the outside
which information the person in question should be able to access. Those are the tasks
which controls which authorizations are to be assigned to the respective role.
Then the relevant business manager or unit manager fills in one
checklist in a document called "Assignment of authorizations, needs and
risk analysis, template: job descriptions and assignments", together with
current employee. The completed list of which purposes a
employees may have a need regarding access to data in TakeCare,
is what constitutes the real need. The operations manager or
the unit manager then places an order to support who executes it
the actual layout of the authorizations in TakeCare.

Unlimited read access is included in all access profiles used by
Aleris Närsjukvård AB in TakeCare, but not necessarily authorization to
establish care documentation.
It is only the executives who actively participate in the care of a patient
who have an access option to personal data in TakeCare. Every
users at Aleris Närsjukvård AB have individual authorizations, incl
own SITHS card and own data account within Aleris Närsjukvård AB. A SITHS card is an e-identification that enables users to identify themselves
with strong authentication when logging into e-services.

All areas within Aleris Närsjukvård AB are laid out as "boxes" which

corresponds to care units. Initially, the user can only read

care documentation within the own "box"/care unit, which in TakeCare

is called a restricted area. An example of a "box"/care unit is the Dalengeriatrician. In this case, the user only sees information

about Dalengeriatriken's patients. Within a "box"/care unit, the user can see everything

information, i.e. all care documentation about the patient. It also applies if

the unit may be divided into smaller units or teams.

If the user works within the care unit "advanced healthcare in the home"

(ASIH) there is the division "north or south". Then the user should only get

authorization to the northern or southern part. If the user needs

authorization in addition to that, e.g. if a doctor works all over

area of operation, he is authorized to do so. The access for

the users within ASIH is limited in such a way that they initially cannot

access data within the geriatric hospitals, or see a list of which

patients who are registered there, unless the manager orders one

competence.

Within the framework of the internal confidentiality, the user himself can through active choices

check boxes that provide access to care documentation at all care units

within Aleris Närsjukvård AB, either because there is consent from

the patient or that it is an emergency. Aleris Närsjukvård AB

does not require the consent of the patient to be documented. The care unit which

the employee has an active service at is preselected.

After an active selection, the user can click on to all information such as

is available about the patient within the framework of internal confidentiality at Aleris

Närsjukvård AB (i.e. to all different care units within Aleris Närsjukvård AB)

in TakeCare. The only information that not all users have access to

refer the sickness certificates to Försäkringskassan. Aleris Närsjukvård AB states that

users are informed that they may not enter journals and read without

be authorized to do so. Aleris Närsjukvård AB considers it a shortcoming that

the company cannot limit within the framework of internal confidentiality

the read authorization between the operations in Aleris Närsjukvård AB.

The only option available to limit access to a care unit is

if the care unit is a so-called protected device. Restrictions can then be made

regarding which other units' records the current care unit's user

can see, and whether users of other healthcare providers should be able to see their records

current care unit. Aleris Närsjukvård AB does not use these

protected units in TakeCare because the company believes that this could

pose a patient safety risk.

Coherent record keeping

Aleris Närsjukvård AB has essentially stated the following.

Needs and risk analysis

There is no specific needs and risk analysis produced for the joint

record keeping.

Authorization assignment regarding access to personal data about patients

Aleris Närsjukvård AB participates in systems for coherent record keeping through

the TakeCare record system and the NPÖ record system, which is a national one

system for coherent record keeping.

Within the framework of coherent record keeping in TakeCare, users can take

part of all care documentation with other care providers included in the system.

Prior to this, the user must first select a specific healthcare provider and then

a dialog box appears. The user must then make an active choice to come

further by clicking in one of two boxes; a box for patient consent

or an emergency box. By clicking in one of the options you get

the user then accesses the specific healthcare provider's records. Aleris

Närsjukvård AB informs users that they are not allowed to access medical records

and read without being authorized to do so.

Through consistent journaling, users can read unlimited what

written on other healthcare providers' units, with the patient's consent, with

exception of if the patient has chosen to block his medical record or if the unit is one

so-called protected device.

If the user wants to access care documentation from another care provider

the user must document that consent has been obtained from the patient.

It is not possible, in terms of authority, for a professional group, to limit that one

only takes part in journals within Aleris Närsjukvård AB.

Due to the fact that the Karolinska University Hospital in an opinion has

stated that there are possibilities to restrict access in TakeCare above

Aleris Närsjukvård AB that the company is aware of the protected units

and that access, through the protected devices, can be restricted within

the framework of the internal secrecy and within the coherent record keeping.

However, Aleris Närsjukvård AB believes that the protected units constitute one

patient safety risk, as restrictions cannot be lifted after

obtained consent from the patients or in emergency situations. Aleris

Närsjukvård AB also believes that it would involve a patient safety risk

if coherent record keeping was opted out. The risk is considered to be extra large

within Aleris Närsjukvård AB's operations because the patients who are cared for

where often have contact with many care providers and thus have a great need

of integrated care.

NPÖ

If a user who has been assigned authorization wants to use NPÖ, they can

this happens in two ways. The user can either go directly into NPÖ and

key in a social security number of your choice which the system then searches for, or so

the user first enters TakeCare and keys in the patient's

social security number and then make a so-called "jump" to that information

which is available about the patient in NPÖ.

Documentation of the access (logs)

Aleris Närsjukvård AB has stated the following.

TakeCare

The documentation shown when extracting the access logs in TakeCare is;

information about the patient, which user has opened the record, which

period of time someone has been inside, all openings of the journal made on it

the patient during the selected period, time and date of the latest

the opening. With regard to which user opened the journal, it is specified

social security number and identification number for the specific unit,
for example ASIH. It also shows which device the user has been on
inside by specifying the specific department of the current care unit.
In the normal log excerpt, it is not clear which actions the user took
has taken or how long someone has been inside the current record, or
which journal entry has been opened, but that information appears
of the in-depth log extracts. The in-depth log extracts are obtained first
after Aleris Närsjukvård AB places an order with Acceptus which in turn
turns to CGM.

NPÖ

The documentation that appears when extracting access logs in NPÖ is;
information about the patient, which user has opened the record, from
which unit the user has been in, for example Dalen geriatrician, date
and time of opening and what actions the user has taken.

Aleris Närsjukvård AB's opinion on the Data Inspectorate's letter

Aleris Närsjukvård AB has comments on the letter Final communication
in view of the decision received by the Swedish Data Protection Authority on March 16, 2020 stated among
other following.

After the Data Inspectorate's inspection, Aleris Närsjukvård AB, together
with certain other actors, took the initiative to and carried out work with
technological changes and improvements in the possibilities of individual
authorization assignments in TakeCare and indirectly in NPÖ. This work has led
to the implementation of new technical solutions at the system supplier which
have now in significant respects corrected the shortcomings of Aleris
Närsjukvård AB which was previously caused by the system's technical limitations.

Aleris Närsjukvård AB further states that another review took place

in 2019 by the Inspectorate for Care and Care (IVO). IVO reviewed
compliance with the law on information security for socially important and
digital services (NIS Act). Part of the review concerned
information security including management of authorizations and
risk work. It is clear from IVO's decision, with regard to authorization allocation
and risk work, the following. "Risk analyzes are also carried out regarding the staff,

for example in connection with employee interviews. Background checks are done
on all employees based on three different levels. Great importance is attached
the authorization control. Internship N.Ä.R.A. AB decides on each
employee's access level to the company's information. Removal of
authorizations when the employment ends are done automatically via a
authorization system." Aleris Närsjukvård AB states that from IVO's final
decision it appears that the company complies in all respects with the NIS Act and that
current directive.
Aleris Närsjukvård AB also states that in connection with the introduction of
data protection regulation and the NIS Act, the company has prioritized routines and
processes within patient safety work highest, followed by ongoing
change work regarding the remaining privacy protection measures. When it
regarding the authorization assignment, it always has, even at
the inspection occasion, characterized by the narrowest possible authority, weighed against
current role/assignment in the company and the need for support in operational and
patient safety considerations required for each position and

duties, taking into account the least possible impact regarding

information security and personal privacy. As previously explained

however, has the technical platform for TakeCare at the time of

the inspection occasion meant that Aleris Närsjukvård AB could not introduce

these limitations fully, which has now been corrected in the system.

Of the submitted basic template used in the needs and risk analysis

it appears that some minor adjustments have taken place. Among other things, it has previously

the question "Which risks would an excessively limited authorization assignment

bring" has been removed and replaced with the question "Anything else?", the answer options

yes and no respectively, followed by a free text box.

Justification of the decision

Applicable rules

The Data Protection Regulation, the primary source of law

The Data Protection Regulation, often abbreviated GDPR, was introduced on May 25, 2018 and

is the primary legal regulation when processing personal data. This

also applies in healthcare.

The basic principles for processing personal data are stated in

Article 5 of the Data Protection Regulation. A basic principle is the requirement of

security according to Article 5.1 f, which states that the personal data must be processed

in a way that ensures appropriate security for the personal data,

including protection against unauthorized or unauthorized processing and against loss,

destruction or damage by accident, using appropriate

technical or organizational measures.

From article 5.2 it appears that the so-called the liability, i.e. that it

personal data controller must be responsible for and be able to demonstrate that the basic

the principles in point 1 are complied with.

Article 24 deals with the responsibility of the personal data controller. Of Article 24.1

it appears that the person in charge of personal data is responsible for carrying out appropriate

technical and organizational measures to ensure and be able to demonstrate that

the processing is carried out in accordance with the data protection regulation. The actions shall

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

and purpose as well as the risks, of varying degree of probability and seriousness, for

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

if necessary.

Article 32 regulates security in connection with processing. According to point 1

must the personal data controller and the personal data assistant with consideration

of the latest developments, implementation costs and treatment

nature, scope, context and purpose as well as the risks, of varying nature

degree of probability and seriousness, for the rights and freedoms of natural persons

take appropriate technical and organizational measures to ensure a

security level that is appropriate in relation to the risk (…). According to point 2 shall

when assessing the appropriate security level special consideration is given to the risks

which the processing entails, in particular from accidental or unlawful destruction,

loss or alteration or to unauthorized disclosure of or unauthorized access to

the personal data transferred, stored or otherwise processed.

Recital 75 states that when assessing the risk of natural persons

rights and freedoms, different factors must be taken into account. Among other things are mentioned

personal data subject to confidentiality, information about health or

sexual life, if there is processing of personal data concerning vulnerable physical

persons, especially children, or if the treatment involves a large number

personal data and applies to a large number of registered users.

Furthermore, it follows from reason 76 that how probable and serious the risk for it

Data subjects' rights and freedoms should be determined based on the processing

nature, scope, context and purpose. The risk should be evaluated on

basis of an objective assessment, through which it is determined whether

the data processing involves a risk or a high risk.

Recitals 39 and 83 also contain writings that provide guidance on it

closer to the meaning of the data protection regulation's requirements for security at

Processing of personal data.

The Data Protection Regulation and the relationship with complementary national

regulations

According to Article 5.1. a in the data protection regulation, the personal data must

processed in a legal manner. In order for the treatment to be considered legal, it is required

legal basis in that at least one of the conditions in Article 6.1 is met.

Provision of health care is one such task of generality

interest referred to in Article 6.1 e.

In healthcare, the legal bases can also be legal

obligation according to Article 6.1 c and exercise of authority according to Article 6.1 e

updated.

When it comes to the question of the legal bases legal obligation, generally

interest and the exercise of authority are given to the Member States, according to Article 6.2, retain or introduce more specific provisions to adapt the application of the provisions of the Regulation to national conditions. National law can further determine specific requirements for data processing and other measures to ensure legal and fair treatment. But there is not only a possibility to introduce national rules but also a duty; Article 6.3 states that the basis for the processing referred to in paragraph 1 c and e shall be determined in accordance with Union law or national law of the Member States. The legal basis may also include special provisions to adapt the application of the provisions of data protection regulation. Union law or Member States' national law right must fulfill an objective of public interest and be proportionate to it legitimate goals pursued.

Article 9 states that treatment of special categories of personal data (so-called sensitive personal data) is prohibited. Sensitive personal data includes, among other things, information about health. Article 9.2 states the exceptions where sensitive personal data may still be processed. Article 9.2 h states that processing of sensitive personal data may take place if the processing is necessary for reasons related to, among other things provision of healthcare on the basis of Union law or Member States' national law or according to agreements with professionals on health area and provided that the conditions and safeguards which

referred to in point 3 are met. Article 9.3 requires regulated confidentiality.

This means that both the legal bases public interest,

exercise of authority and legal obligation such as treatment of sensitive

personal data with the support of the exception in Article 9.2. h needs

supplementary rules.

Supplementary national regulations

For Swedish purposes, both the basis for the treatment and the

the special conditions for processing personal data within health and

healthcare regulated in the Patient Data Act (2008:355) and

the patient data regulation (2008:360). In ch. 1 Section 4 of the Patient Data Act states that

the law supplements the data protection regulation.

The purpose of the Patient Data Act is that information management within health and

healthcare must be organized so that it caters for patient safety and

good quality and promotes cost efficiency. Its purpose is also to

personal data must be designed and otherwise processed so that patients' and

the privacy of other data subjects is respected. In addition, must be documented

personal data is handled and stored so that unauthorized persons do not gain access

them (Chapter 1, Section 2 of the Patient Data Act).

The supplementary provisions in the Patient Data Act aim to

take care of both privacy protection and patient safety. The legislature has

thus, through the regulation, a balance has been made in terms of how

the information must be processed to meet both the requirements for patient safety

such as the right to personal integrity in the processing of personal data.

The National Board of Health and Welfare has issued regulations with the support of the patient data regulation and general advice on record keeping and processing of personal data i health care (HSLF-FS 2016:40). The regulations constitute such supplementary rules, which must be applied when healthcare providers treat personal data in healthcare, see ch. 1 Section 1 of the Patient Data Act.

National regulations that supplement the data protection regulation's requirements for security can be found in chapters 4 and 6. the Patient Data Act and chs. 3 and 4 HSLF-FS 2016:40.

Requirement to carry out a needs and risk analysis

The care provider must according to ch. 4. § 2 HSLF-FS 2016:40 make a need-and risk analysis, before assigning authorizations in the system takes place.

That an analysis of the needs as well as the risks is required is evident from the preparatory work to the Patient Data Act, prop. 2007/08:126 pp. 148-149, as follows.

Authorization for the staff's electronic access to information about patients must be limited to what the executive needs to be able to perform his duties in health and healthcare. It includes, among other things, that authorizations must be followed up and changed or restricted accordingly hand as changes in the individual executive's duties give rise to it.

The provision corresponds in principle to Section 8 of the Care Register Act. The purpose of the provision is to inculcate the duty of the responsible health care provider to make active and individual authorization assignments based on analyzes of which detailed information different personnel categories and different types of operations need. But it is not only necessary needs analyses. Risk analyzes must also be carried out where different types of risks are taken into account such as may be associated with excessively wide availability regarding certain types of information.

Protected personal data marked confidential, information about publicly known persons, data from certain clinics or medical specialties are examples of categories such as

may require special risk assessments.

Generally speaking, it can be said that the more extensive an information system is, the greater the quantity

different authorization levels there must be. Decisive for decisions on eligibility for e.g. various

categories of healthcare professionals to electronic access to records i

patient records should be that the authorization should be limited to what the executive needs

for the purpose of good and safe patient care. A more extensive or coarse meshed

authorization assignment should - even if it would have points from an efficiency point of view - be considered as an unjustified

dissemination of medical records within an activity and as such should

not accepted.

Furthermore, data should be stored in different layers so that more sensitive data requires active choices or

otherwise are not as easily accessible to staff as less sensitive information. When it

applies to personnel who work with operational follow-up, statistical production, central

financial administration and similar activities that are not individual-oriented, probably

the majority of executives have access to information that can only be derived indirectly

to individual patients. Electronic access to code keys, social security numbers and others

information that directly points out individual patients should be able to be strong in this area

limited to single persons.

Internal confidentiality

The provisions in ch. 4 The Patient Data Act concerns internal confidentiality, i.e.

regulates how privacy protection must be handled within a healthcare provider's operations

and especially employees' opportunities to prepare access to

personal data that is electronically available in a healthcare provider's

organisation.

It appears from ch. 4. Section 2 of the Patient Data Act, that the healthcare provider must decide

conditions for granting authorization to access such information about

patients who are transported fully or partially automated. Such authorization shall

is limited to what is needed for the individual to be able to fulfill their duties

tasks within health care.

Of ch. 4 § 2 HSLF-FS 2016:40 follows that the care provider must be responsible for each

users are assigned an individual authorization for access to

personal data. The healthcare provider's decision on the allocation of authorization shall

preceded by a needs and risk analysis.

Coherent record keeping

The provisions in ch. 6 the Patient Data Act concerns coherent record keeping,

which means that a care provider – under the conditions stated in § 2 hereof

chapter - may have direct access to personal data processed by others

care provider for purposes related to care documentation. Access to

information occurs through a healthcare provider making the information about a patient

which the healthcare provider registers about the patient available to other healthcare providers

who participate in the integrated record keeping system (see prop. 2007/08:126

p. 247).

Of ch. 6 Section 7 of the Patient Data Act follows that the regulations in ch. 4 Sections 2 and 3 also apply to authorization

assignment and access control in the event of a joint operation

record keeping. The requirement that the healthcare provider carry out a needs and risk analysis

before the assignment of authorizations in the system takes place, thus also applies in systems

for consistent record keeping.

Documentation of access (logs)

Of ch. 4 Section 3 of the Patient Data Act states that a healthcare provider must ensure that

access to such patient data that is held in whole or in part

automatically documented and systematically checked.

According to ch. 4 § 9 HSLF-FS 2016:40 the care provider must be responsible for

1. it is clear from the documentation of the access (logs) which

actions taken with data about a patient;

2. the logs show which care unit or care process

the measures have been taken,

3. it is clear from the logs at which time the measures were taken,

4. the identity of the user and the patient can be seen from the logs.

The Swedish Data Protection Authority's assessment

Personal data controller's responsibility for security

As previously described, it is stated in article 24.1 of the data protection regulation one

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement partly aims to ensure that

the processing of the personal data is carried out in accordance with

the data protection regulation, partly that the person in charge of personal data must be able to

show that the processing of the personal data is carried out in accordance with

data protection regulation.

The security in connection with the treatment is regulated more specifically in the articles

5.1 f and 32 of the data protection regulation.

Article 32.1 states that the appropriate measures must be both technical and

organizational and they must ensure a level of security that is appropriate in

relation to the risks to the rights and freedoms of natural persons which
the treatment entails. It is therefore necessary to identify the possible ones
the risks to the rights and freedoms of the data subjects and assesses
the likelihood of the risks occurring and the severity if they occur.
What is appropriate varies not only in relation to the risks but also
based on the nature, scope, context and purpose of the treatment. It has
thus meaning what kind of personal data is processed, how many
data it is a question of, how many people process the data, etc.
Health care has a great need for information in its operations. The
it is therefore natural that the possibilities of digitization are utilized as much as possible
possible in healthcare. Since the Patient Data Act was introduced, one has a lot

extensive digitization has taken place in healthcare. As well as the data collections
size as how many people share information with each other has increased
substantially. This increase means at the same time that the demands on it increase
personal data controller, because the assessment what is an appropriate
safety is affected by the extent of processing.
There is also the issue of sensitive personal data. The information concerns
people who are in a dependent situation when they are in need of care.
It is also often a question of a lot of personal data about each of these
people and the data may over time be processed by very
many people in healthcare. All in all, this places great demands on it
personal data controller.

The data that is processed must be protected against external actors as well
the business as against unauthorized access from within the business. It appears
of article 32.2 that the personal data controller, when assessing the appropriate
security level, in particular must take into account the risks of accidental or illegal
destruction, loss or for unauthorized disclosure or access. In order to
able to know what is an unauthorized access it must
personal data controller is clear about what constitutes an authorized access.

Needs and risk analysis

In ch. 4 § 2 The National Board of Health and Welfare's regulations (HSLF-FS 2016:40), which supplement
the patient data act, it is stated that the care provider must make a needs assessment
risk analysis before assigning authorizations in the system takes place. This means that
national law prescribes requirements for an appropriate organizational measure that shall
is taken before assigning authorizations to the record system takes place.

A needs and risk analysis must partly contain an analysis of the needs, partly a
analysis of the risks based on an integrity perspective that may be associated
with an excessively wide allocation of authorization for access to personal data
about patients. Both the needs and the risks must be assessed based on them
information that needs to be processed in the business, what processes it is
the question of whether and what risks exist for the individual's privacy.

The assessments of the risks need to take place based on organizational level, there
for example, a certain part of the business or task may be more
more sensitive to privacy than another, but also based on the individual level, if that is the case
the question of special circumstances that need to be taken into account, such as for example

that it is a matter of protected personal data, generally known persons or

otherwise particularly vulnerable persons. The size of the system also affects

the risk assessment. It appears from the preparatory work for the Patient Data Act that the more

comprehensive an information system is, the greater the variety

authorization levels must exist (prop. 2007/08:126 p. 149).

It is thus a question of a strategic analysis at a strategic level, which should provide

an authorization structure that is adapted to the business and this shall

be kept up to date.

In summary, the regulation requires that the risk analysis identifies

- different categories of data,
- categories of data subjects (for example, vulnerable natural persons and children), or
- the extent (for example, the number of personal data and registered)
- negative consequences for data subjects (e.g. damages, significant social or economic disadvantage, deprivation of rights and freedoms),

and how they affect the risk to the rights and freedoms of natural persons at

Processing of personal data. This also applies to internal confidentiality

as with coherent record keeping.

The risk analysis must also include special risk assessments, for example

based on whether there are protected personal data that are

classified as confidential, information about publicly known people, information from certain receptions or medical specialties (prop. 2007/08:126 p. 148149).

The risk analysis must also include an assessment of how likely and how serious the risk to the rights and freedoms of the data subjects is based on the nature, scope, context and purpose of the processing (reason 76).

It is thus through the needs and risk analysis that it data controller finds out who needs access, which data the access possibility must include, at which times and in which context the access is needed, and at the same time analyzes the risks to it individual freedoms and rights that the processing may lead to. The result shall then lead to the technical and organizational measures needed to

ensure that no other access than that which is necessary and the risk analysis shows is justified should be able to take place.

When a needs and risk analysis is missing prior to granting authorization i system, there is no basis for the personal data controller on a legal basis way must be able to assign their users a correct authorization. The personal data controller is responsible for, and must have control over, it personal data processing that takes place within the scope of the business. To assign users a case of access to the record system, without this being founded on a performed needs and risk analysis, means that the personal data controller does not have sufficient control over the personal data processing that takes place in the record system and also cannot show that he has the control that

is required.

When the Swedish Data Protection Authority has requested a documented need and risk analysis, Aleris Närsjukvård AB has referred to the document Assignment of authorizations, needs and risk analysis, template: Functional descriptions and mission. The document states that the responsible manager must carry out a needs and risk analysis when hiring an employee based on the employee's needs authorizations to access personal data and that the assessment is made based on tasks and workplace. Regarding the risk analysis of a employees to be hired, this consists of one question - "Which risks would does an overly limited authority assignment entail?" Prior to the award of an authorization profile, it is stated that risks and needs must be weighed. The privacy risk addressed in the document also consists of a question – "Which risks regarding patient integrity does this mean that the authorization is given?" The the only suggestion of risk given is "risk of access by, for the treatment occasion, no necessary patient data in TakeCare through the possibility to coherent record keeping".

As indicated above, in a needs and risk analysis both the needs and the risks are assessed based on the information that needs to be processed in the business, which processes it is a question of and which risks to it individual integrity that exists both organizationally and individually level. It is thus a question of a strategic analysis at a strategic level, which must provide an authorization structure that is adapted to the operations. It should result in authorization assignment instructions but it is not the instructions to the assigner of permissions which is the analysis.

During the Data Inspectorate's review, Aleris Närsjukvård AB has not been able to demonstrate any need and risk analysis - whether within the framework of the internal confidentiality or within the framework of coherent record keeping. Aleris Närsjukvård AB's documents lack the basic inventory of users' needs for access and risk analysis, and it has not some balance has been made between needs and the actual privacy risks that the processing of personal data gives rise to

In its analysis, Aleris Närsjukvård AB has not considered negative consequences for data subjects, different categories of data, categories of data subjects, or the extent of the number of personal data and data subjects affects the risk of the rights and freedoms of natural persons of Aleris Närsjukvård AB: s processing of personal data in TakeCare and NPÖ. It is also missing special risk assessments based on whether there is e.g. protected personal data marked confidential, information about public knowledge persons, data from certain receptions or medical specialties or other factors that require special protective measures. It is also missing assessment of how probable and serious the risk to those registered rights and freedoms are judged to be.

In summary, the Data Inspectorate states that the documents Assignment of authorizations, needs and risk analysis, template: Job Descriptions and Assignments, Assessment of Access Privileges to information about patients as well as to other systems and Authorization roles/profiles in patient data systems, which have been reported by Aleris Närsjukvård AB does not meet the requirements set for a need and

risk analysis and that Aleris Närsjukvård AB has not been able to demonstrate that they

carried out a needs and risk analysis in the sense referred to in ch. 4. Section 2

HSLF-FS 2016:40, whether within the framework of internal secrecy or within

the framework for the coherent record-keeping, according to ch. 4 and 6, respectively.

the patient data act. This means that Aleris Närsjukvård AB has not taken any measures

appropriate organizational measures in accordance with Article 5.1 f and Article 31.1

and 31.2 to be able to ensure and, in accordance with Article 5.2, to be able to demonstrate

that the processing of the personal data has a security that is suitable i

relation to the risks.

Authorization assignment regarding access to personal data about patients

As has been reported above, a care provider may have a legitimate interest in having

a comprehensive processing of information about the health of individuals. Regardless of this shall

access possibilities to personal data about patients be limited to

what is needed for the individual to be able to fulfill his duties.

Regarding the assignment of authorization for electronic access according to ch. 4.

§ 2 and ch. 6 Section 7 of the Patient Data Act, it appears from the preliminary works, prop.

2007/08:126 pp. 148-149, i.a. that there must be different authorization categories in

the journal system and that the authorizations must be limited to what the user

need to provide the patient with good and safe care. It also appears that "one

more extensive or coarse-grained authority assignment should be considered a

unjustified dissemination of medical records within a business and should as

such is not accepted."

In healthcare, it is the person who needs the data in their work
who may be authorized to access them. This applies both within a
caregivers as between caregivers. It is, as already mentioned, through
the needs and risk analysis that the personal data controller finds out about whom
who needs access, which data the access should cover, at which
times and in which contexts the access is needed, and at the same time
analyzes which risks to the individual's freedoms and rights are
the treatment can lead to. The result should then lead to the technical and
organizational measures needed to ensure that no allocation
of authorization provides further access possibilities than the one that needs and
the risk analysis shows is justified. An important organizational action is to give
instructions to those who have the authority to assign permissions on how to do this
should go to and what should be taken into account so that, with the needs and risk analysis
as a basis, will be a correct authorization assignment in each individual case.
According to Aleris Närsjukvård AB, there is an opportunity to limit users' rights
access to patients' information, within the framework of internal confidentiality, i
TakeCare through the so-called protected devices. Aleris Närsjukvård AB
however, has not introduced such units. The only restriction on access that
available in the system relate to the sickness certificates to Försäkringskassan, which not all of them
users have access to.
Aleris Närsjukvård AB has expressed it as the authorizations in the interior
privacy is to some extent limited by so-called active choices, which means that
the user can initially only read care documentation within their own
the "box"/care unit. Within a "box"/care unit, the user can see everything
information, i.e. all care documentation about the patient. It also applies if

the unit may be divided into smaller units or teams. Within the framework of it
internal privacy, the user can tick boxes themselves through active choices
provides access to care documentation at all care units within Aleris
Närsjukvård AB, either because there is consent from the patient
or that it is an emergency.

When it comes to accessing data within a healthcare provider's business, so
it follows from ch. 4. § 4 HSLF-FS 2016:40 that the care provider "shall be responsible for
information about which other care units or in which other care processes
there is information about a particular patient that cannot be made available without it
the authorized user has made a decision as to whether he or she has
right to access this information (active choice). The data then does not get
are made available without the authorized user making another active
choice."

Aleris Närsjukvård AB uses active elections according to ch. 4. Section 4 HSLF-FS 2016:40.
It is in and of itself an integrity-enhancing measure. However, this does not mean that
the possibility of access to personal data in the system has been restricted for
the user in such a way that they are no longer accessible, but the data is
still electronically accessible. By the user clicking in the box for
consent or emergency access, he can still share with everyone
personal data, which means that all users who make these active choices
can access the patients' data and not only the users who have
a need. This means that the active choices are not such
access restriction referred to in ch. 4 Section 2 of the Patient Data Act. This one

provision requires that the authorization be limited to what is needed for

that the individual must be able to fulfill his duties within health and

healthcare, i.e. only those who need the information should be able to have it

access to them.

Aleris Närsjukvård AB has also not introduced any restrictions within the framework

for the coherent record keeping in the TakeCare system, even if it

there are options for the care provider to limit the user's access to

personal data of other healthcare providers.

Regarding access to personal data about patients within the framework of it

coherent record keeping in the NPÖ system has 335 users at Aleris

Närsjukvård AB granted authorization. The Swedish Data Protection Authority can state that

a limitation has been made regarding the number of users, based on the 1,700

users who are at Aleris Närsjukvård AB, but it is not clear why

335 out of 1700 employees have been given this access option. It also appears

not that there has been any limitation of which documentation these

users can take part in NPÖ.

According to Aleris Närsjukvård AB, the user can either go directly into NPÖ

and key in a social security number of your choice, which the system then searches for,

or the user first enters TakeCare and keys in the patient's

social security number and then make a jump to the information available

about the patient in NPÖ.

Because different users have different tasks within different

work areas, users' access to the record systems needs to be restricted

to reflect this. Aleris Närsjukvård AB has not limited the users

authorizations for access to patients' personal data in the records system,

either within the framework of the internal confidentiality of the TakeCare system or within

the framework for the coherent record keeping in the TakeCare and NPÖ systems.

This means that a majority of users have had actual access to

a majority of patients' personal data in TakeCare. In the system NPÖ has

all 335 users had access to the personal data being processed

within the framework of NPÖ.

That the assignment of authorizations has not been preceded by a need-and

risk analysis means that Aleris Närsjukvård AB has not analyzed the users

need for access to the data, the risks that this access may entail

and thus also not identifying which access is warranted

the users based on such an analysis. Aleris Närsjukvård AB therefore does not have

used appropriate measures, in accordance with Article 32

data protection regulation, to limit users' access to

the patients' personal data in the record system. This in turn has meant

that there was a risk of unauthorized access and unauthorized dissemination of

personal data partly within the framework of internal confidentiality, partly within the framework

for the coherent record keeping.

In light of the above, the Swedish Data Protection Authority can state that Aleris

Närsjukvård AB has processed personal data in violation of article

5.1 f and article 32.1 0ch 32.2 of the data protection regulation by Aleris

Närsjukvård AB has not limited the user's permissions for access to

the record system TakeCare and NPÖ to what is only needed to

the user must be able to fulfill his tasks within health and

healthcare according to ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and ch. 4 Section 2 HSLF-FS 2016:40. This means that Aleris Närsjukvård AB has not taken any measures measures to be able to ensure and, in accordance with Article 5.2 i data protection regulation, be able to demonstrate a suitable security for the personal data.

Documentation of the access (logs)

The Swedish Data Protection Authority can state that from the logs in TakeCare and NPÖ information about the specific patient, which user has opened the journal, actions taken, which journal entry has been opened, what time period the user has been in, all openings of the record made on that patient during the selected time period and time and date of last opening.

Datainspektionen has nothing to recall in this part, because the documentation of the access (logs) in TakeCare and NPÖ is in compliance with the requirements set out in ch. 4. Section 9 HSLF-FS 2016:40 and has thereby taken appropriate technical measures in accordance with Article 32 i data protection regulation.

Statement on the Swedish Data Protection Authority's letter Final communication after decision

Aleris Närsjukvård AB has supplemented its previous tasks with one statement received by the Data Protection Authority on March 16, 2020, where Aleris Närsjukvård AB states that it has conducted work with technical changes and improvements to the opportunities for individual

authorization assignments in TakeCare and indirectly in NPÖ. The work has led to implementation of new technical solutions at the system supplier which have now in significant respects corrected the shortcomings of Aleris Närsjukvård AB which was previously prompted by the system's technical limitations.

Aleris Närsjukvård AB also states that it appears from IVO's final decision that the company in all respects complies with the NIS Act and the current directive, among other things regarding the management of authorizations and risk work.

The Swedish Data Protection Authority considers it positive that Aleris Närsjukvård AB has contributed to the fact that there have been implementations in the form of new technical solutions in TakeCare, which has corrected deficiencies at Aleris Närsjukvård AB. However, it does not appear what these deficiencies are or in what way the deficiencies has been corrected within the framework of Aleris Närsjukvård AB's allocation of permissions.

The Swedish Data Protection Authority can further state that IVO's review of Aleris Närsjukvård AB is based on provisions in the Act (2018:1174) on information security for socially important and digital services (NIS Act) and the applicable directive, and not based on the data protection regulation and the provisions of the Patient Data Act. The NIS Act aims to achieve a high level on the security of the networks and information systems for important public entities services while data protection regulations aim to protect them were registered freedoms and rights when processing personal data.

Choice of intervention

Legal regulation

If there has been a breach of the data protection regulation has

Datainspektionen a number of corrective powers to be available according to article

58.2 a - j of the data protection regulation. The supervisory authority can, among other things

order the personal data controller to ensure that the processing takes place in

in accordance with the regulation and if required in a specific manner and within a

specific period.

It follows from Article 58.2 of the data protection regulation that the Data Inspectorate i

in accordance with Article 83 shall impose penalty charges in addition to, or in lieu of,

other corrective measures referred to in Article 58(2), depending

the circumstances of each individual case.

Article 83(2) sets out the factors to be taken into account in deciding whether a

administrative penalty fee shall be imposed, but also what shall affect

the amount of the penalty fee. Of central importance for the assessment of

the seriousness of the breach is its nature, severity and duration. If

it is a question of whether a minor violation gets the supervisory authority, according to reason

148 of the Data Protection Regulation, issue a reprimand instead of imposing one

penalty fee.

Order

Health care has, as mentioned, a great need for information in its

Operation. It is therefore natural that the possibilities of digitization

taken care of as much as possible in healthcare. Since the Patient Data Act

was introduced, a very extensive digitization has taken place in healthcare. Both

the data collections size as how many people share information with

each other have increased significantly. This increase means at the same time that the requirements increases on the personal data controller, because the assessment what is a appropriate security is affected by the extent of processing.

Within health care, this means a great deal of responsibility for it personal data controller to protect the data from unauthorized access, among other things by having an authorization assignment that is even more finely divided. It is therefore essential that there is a real analysis of the needs based on different businesses and different executives. Equally important is that there is an actual analysis of the risks based on an integrity perspective can occur in the event of an excessive assignment of authorization to access. From this analysis must then be limited to the individual executive's access. This authorization must then be followed up and changed or restricted accordingly hand that changes in the individual executive's duties provide reason for it.

The Data Inspectorate's supervision has shown that Aleris Närsjukvård AB has not taken any measures appropriate security measures to protect the personal data in TakeCare and NPÖ by not complying with the requirements set out in the Patient Data Act and The National Board of Health and Welfare's regulations and thereby does not meet the requirements in article 5.1 f and Article 32.1 and 32.2 of the data protection regulation. The omission covers both the internal secrecy according to ch. 4 the patient data act as it coherent record keeping according to ch. 6 the patient data act.

The Swedish Data Protection Authority therefore orders, with the support of Article 58.2 d i the data protection regulation, Aleris Närsjukvård AB to implement and document the required needs and risk analysis for the record systems

TakeCare and NPÖ within the framework of both internal confidentiality and within
the framework for the coherent record keeping. Aleris Närsjukvård AB shall
further, with the support of the needs and risk analysis, assign each user
individual authorization for access to personal data which is limited to
only what is needed for the individual to be able to fulfill their duties
tasks within health care.

Penalty fee

The Swedish Data Protection Authority can state that the violations basically relate to Aleris
Närsjukvård AB's obligation to take appropriate security measures to provide
protection of personal data according to the data protection regulation.

In this case, it is a matter of large collections of sensitive data
personal data and extensive permissions. The caregiver needs to
necessity to have extensive processing of information about individuals' health.
However, it must not be unrestricted, but must be based on what individuals do
employees need to be able to perform their tasks. The Swedish Data Protection Authority
states that it is a matter of data that includes direct identification
of the individual through both name, contact details and social security number,
information about health, but it can also be about other private information
about, for example, family relationships, sex life and lifestyle. The patient is
dependent on receiving care and is thus in a vulnerable situation. of the data
nature, extent and the patients' dependency status give caregivers a
particular responsibility to ensure patients' right to adequate protection for their

personal data.

Further aggravating circumstances are that the treatment of

personal data about patients in the main record system is at the core of a

care provider's activities, that the treatment includes many patients and

the possibility of access concerns a large percentage of the employees. Within the scope of

the internal secret service has 1,700 people access to information relating to

around 55,000 patients, apart from the information relating to the sick certificates

The Swedish Social Insurance Agency, which not all users have access to. In addition,

the possibility of access for the 1,700 people to the personal data within

the framework for the coherent record keeping through TakeCare and the 335

users who have access to the large data collections in NPÖ.

It is a central task for the personal data controller to take measures

to ensure an appropriate level of security in relation to the risk. At

the assessment of the appropriate security level must take special account of the risks

which the processing entails, in particular from accidental or unlawful destruction,

loss or alteration or to unauthorized disclosure of or unauthorized access to

the personal data transferred, stored or otherwise processed,

according to article 32.2 of the data protection regulation. The requirements for health and

the healthcare area, currently applicable security measures, have been specified in

the Patient Data Act and regulations in the National Board of Health and Welfare. Of the preparatory work to

The Patient Data Act clearly states that requirements are placed on strategic analysis as well as

that authority allocation takes place individually and is adapted to the current one

the situation. That Aleris Närsjukvård AB has assigned authorizations without

complying with these requirements means that the action took place intentionally and is therefore assessed

as more serious.

When determining the seriousness of the violations, it can also be established that the violations also include the fundamental principles of Article 5 i the data protection regulation, which is among the more serious violations that can give a higher penalty fee according to Article 83.5 of the Data Protection Regulation. Taken together, these factors mean that the violations cannot be assessed as minor infractions without infractions that should lead to one administrative penalty fee.

The Swedish Data Protection Authority believes that these violations are closely related to each other. That assessment is based on the fact that the needs and risk analysis must form the basis for the assignment of the authorizations. The Swedish Data Protection Authority therefore considers that these violations are so closely related to each other that they constitute connected data processing according to Article 83.3 i data protection regulation. The Swedish Data Protection Authority therefore determines a joint penalty fee for these violations.

According to Article 83.3, the administrative sanction fee may not exceed the amount of the most serious violation if it is one or the same data processing or connected data processing.

The administrative penalty fee must be effective, proportionate and deterrent. This means that the amount must be determined so that it the administrative sanction fee leads to correction, that it provides a preventive measure effect and that it is also proportionate in relation to current as well violations as to the solvency of the subject of supervision.

As regards calculation of the amount, Article 83.5 i

data protection regulation that companies that commit violations such as those in question
may be subject to penalty fees of up to twenty million EUR or four
percentage of the total global annual turnover in the previous financial year,
depending on which value is the highest.
The term company includes all companies that conduct an economic
business, regardless of the entity's legal status or the manner in which it
be financed. A company can therefore consist of an individual company in the sentence one
legal person, but also by several natural persons or companies. Thus
there are situations where an entire group is treated as a company and its

total annual turnover shall be used to calculate the amount of a
breach of the Data Protection Regulation by one of its companies.
From consideration reason 150 in the data protection regulation appears, among other things
following. […] If the administrative penalty charges are imposed on a company,
should a company for this purpose be deemed to be a company within the meaning of
Articles 101 and 102 of the TFEU[…]. This means that the assessment of
what constitutes a company must be based on the definitions of competition law.
The rules for group liability in EU competition law revolve around
the concept of economic unity. A parent company and a subsidiary company are considered
as part of the same economic entity when the parent company exercises one
decisive influence over the subsidiary. The Swedish Data Protection Authority therefore puts
as a starting point the turnover for Aleris Group AB as a basis for
the calculation of the amount of the penalty fee.

Aleris Group AB was formed at the end of 2019. Some turnover figures for the whole 2019 is therefore not available. There is therefore no information on the annual turnover for determining the size of the penalty fee. Aleris Närsjukvård AB has stated that the group turnover for Aleris Group AB amounted to just over SEK 1.2 billion between 1 October 2019 and 31 December 2019. Converted for a full year, it would correspond to a turnover of approximately SEK 4.9 billion.

The Data Inspectorate states that because Provliva AB and associated subsidiaries (including Aleris Närsjukvård AB) were bought out and then on 1 April 2020 has Aleris Group AB as the group parent, it is likely that it the actual annual turnover for Aleris Group AB in the current year will be significantly higher.

In the current case, the Data Protection Authority applies a precautionary principle and therefore estimates that the company's annual turnover at least corresponds to that of the period October – December 2019 recalculated for a full year, i.e. approximately 4.9 billion kroner. The highest sanction amount that can be established in current case is EUR 20,000,000, which is roughly four percent of the company's estimate revenue.

In light of the seriousness of the violations and that the administrative the penalty fee must be effective, proportionate and dissuasive

The Swedish Data Protection Authority determines the administrative penalty fee for Aleris Närsjukvård AB to SEK 12,000,000 (twelve million).

This decision has been made by the director general Lena Lindgren Schelin after

presentation by IT security specialist Magnus Bergström. At the final

Chief legal officer Hans-Olof Lindblom, the unit managers are also involved in the handling

Katarina Tullstedt and Malin Blixt and the lawyer Linda Hamidi participated.

Lena Lindgren Schelin, 2020-12-02 (This is an electronic signature)

Appendix

How to pay penalty fee

Copy for information

The data protection officer

How to appeal

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

the letter which decision you are appealing and the change you are requesting.

The appeal must have been received by the Swedish Data Protection Authority no later than three weeks from

the day you were informed of the decision. If the appeal has been received in time

the Swedish Data Protection Authority forwards it to the Administrative Court in Stockholm for

examination.

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain

any privacy-sensitive personal data or information that may be covered by

secrecy. The authority's contact details appear on the first page of the decision.