Decision

Diarienr

2020-12-02

DI-2019-3842

Aleris Närsjukvård AB

Box 6401

113 82 Stockholm

Stockholm County

Supervision under the Data Protection Regulation and

Patient Data Act- needs and risk analysis and

questions about access in journal systems

Table of Contents

The Data Inspectorate's decision

During the inspection on 24 April 2019, the Data Inspectorate 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

Phone: 08-657 61 00

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

the Data Protection Regulation1 by

1.

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

before authorization is granted in the TakeCare medical record system

and National Patient Overview (NPÖ) in accordance with ch. § 2 and

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

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

and processing of personal data in health care. This

means that Aleris Närsjukvård AB has not taken appropriate

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

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

in relation to the risks.

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

access to the journal system TakeCare and NPÖ to what only

needed for the user to be able to fulfill his tasks

in health and medical care in accordance with ch. § 2 and ch. 6 § 7

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

Aleris Närsjukvård AB has not taken any measures to be able to

ensure and be able to show appropriate security for personal data.

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

the Data Protection Ordinance that Aleris Närsjukvård AB for the violations

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

the Data Protection Regulation shall pay an administrative penalty fee of

SEK 12,000,000 (twelve million).

The Data Inspectorate submits pursuant to Article 58 (2) (d) i

data protection ordinance Aleris Närsjukvård AB to implement and

document the required needs and risk analysis for the journal systems

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

assign each user individual privileges to access

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

individuals must be able to fulfill their duties in health 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 information and repealing Directive 95/46 / EC (General Data Protection Regulation).

in accordance with Article 5 (1) (f) and Article 32 (1) and (2) of the Data Protection Regulation; Chapter 4 § 2 and ch. 6 Section 7 of the Patient Data Act and Chapter 4 2 § HSLF-FS 2016: 40.

Report on the supervisory matter

The Data Inspectorate initiated the inspection by letter dated 22 March 2019 and has on site on 24 April 2019 reviewed whether Aleris Närsjukvård AB's decision on allocation of authorizations has been preceded by a needs and risk analysis. The review also included how Aleris Närsjukvård AB allocated permissions for accessing the TakeCare and NPÖ master journal system, and what access possibilities the granted privileges provide within both the framework 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 examined the documentation of access (logs) contained in the journal systems.

The Data Inspectorate has only examined users' access possibilities to journal systems, i.e. what care documentation the user can actually take part of and read. Supervision does not include the functions included in the competence, ie. what the user can actually do in the journal systems (eg issuing prescriptions, writing referrals, etc.).

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

What has emerged in the case

Aleris Närsjukvård AB has mainly stated the following.

The responsibility for personal data

Aleris Närsjukvård AB is responsible for personal data and care providers.

The business

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

The Data Inspectorate with information that Praktikertjänst N.Ä.R.A. AB

divested from the Praktikertjänst Group (corporate identity number 556077-2419) on 1 April

2020 and changed its name to Aleris Närsjukvård AB (corp. No. 556743-1951). With

Due to this, the Data Inspectorate requested additional information

from Aleris Närsjukvård AB. The additions show, among other things

following.

On 1 October 2019, Aleris Healthcare AB (corporate identity number 556598-6782) will be acquired

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

Group parent company, Aleris Group AB (corporate identity number 559210-7550).

On 1 April 2020, Proliva AB (corp. No. 556472-1958) and associated products will be purchased

subsidiary of Triton. Proliva AB receives Aleris Group AB as

group mother.

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

percent of Provliva AB. Provliva AB was in turn one hundred percent owned by

the group parent company Praktikertjänst AB.

Following the divestment on April 1, 2020, Aleris Närsjukvård AB will continue to own one

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

Proliva AB is in turn 100% owned by Aleris Healthcare AB.

The Group parent company for the entire “Aleris Group”, including the “Proliva Group”, is Aleris Holding AB (corporate identity number 559210-7535).

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

Group sales for Aleris Group AB amounted to SEK 1,215,385,000 between October 1, 2019 and December 31, 2019. Since Aleris Group AB was formed in connection with the change of ownership when Aleris Healthcare AB joined 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 medical record system within framework of internal confidentiality and participates in TakeCare's system for coherent record keeping. TakeCare has been used by Aleris Närsjukvård AB since 2009. Digital journals 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 introduction of medical records. Over the years, Aleris Närsjukvård AB has follow-up meetings with CompuGroup Medical (CGM), which is a provider of

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

competencies, and the 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 unified record keeping.

The number of patients and employees

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

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

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

Internal secrecy

Needs and risk analysis

Aleris Närsjukvård AB has mainly stated the following.

There is a template for needs and risk analysis, Allocation of authorizations,

needs and risk analysis, template: Functional descriptions and assignments, and that is

operations managers and unit managers who are to perform needs and

the risk analysis before assigning authorizations in the systems.

The template shows i.a. that risks and needs must be weighed before allocating

a competency profile and that it is the responsible manager who performs a needs and

risk analysis of the employee's need for access rights to

personal data. The assessment is made on the basis of tasks and

workplace. If the employee needs access to TakeCare for

For the purpose of "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

the authority is given? (justify in the form of access to patient data) ”. The

There are two statements that can be crossed out:

-

Opportunity to actively choose to open another journal within

the restricted area (the care area) through its competence (lift internally

confidentiality) ”, or

-

“Risk of access to, at the time of care, unnecessary patient data

in TakeCare through the possibility of cohesion

journal / reading permission ”.

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

There is a routine that is linked to the template, Assessment of permissions for access to patient data as well as to other systems, and that routine is stated to constitute instruction to the head of operations and the head of unit how he shall proceed in the allocation of authorizations. The routine shows that permissions to electronic systems that contain patient data shall limited to what is needed for the employee to be able to fulfill theirs tasks in healthcare. Furthermore, it appears that the boss, in connection with a new employees' access to employment, make an assessment of which permissions the new employee needs. There are no more instructions, but instead refers to another document.

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

There is no "complete answer template" for what a risk analysis should look like, but the risk analysis consists of the current head of operations or unit head doing one assessment which it can then write down in a free text box in the document Allocation of authorizations - needs and risk analysis, template: Functional descriptions and assignments.

The head of operations or the head of unit must answer the question in the template which reads:

"What risks would an overly limited allocation of privileges entail?"

Examples of responsible manager's risk analyzes when it comes to whether employees have

needs for access to data in TakeCare are:

- “No need based on patient safety that the employee has

authorization in TC or other patient-related systems ”.

- “Reduced accessibility for patients when collaboration takes place with both

geriatrics such as ASIH and SPSV to make optimal use of personnel

resources. Reduced continuity for patients or risk of

patient-insecure record keeping of drug administration. "

- “Complicate patient work and prevent the possibility of being helped

to maintain accessibility for patients at work peaks or

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

ASIH team ”.

Authorization assignment for access to personal data

Aleris Närsjukvård AB has mainly stated the following.

Aleris Närsjukvård AB uses the company Acceptus developed

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

Based on the permissions included in these templates

Aleris Närsjukvård AB has made its own list of different qualifications and needs

as the roles have.

The authorization allocation is largely done in the following way. In a first layer

is the "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. "Hand geriatrics" and in the third layer, permission is added from the outside

what information the person in question should be able to take part in. These are the tasks

which governs which competencies are to be assigned to each role.

Then the current operations manager or unit manager fills in one

checklist in a document called “Allocation of permissions, needs and

risk analysis, template: job descriptions and assignments ”, together with

current employee. The completed list of what purposes one

employees may need access to data in TakeCare,

is what constitutes the real need. Operations Manager or

the unit manager then places an order with the support that performs it

the actual structure of the permissions in TakeCare.

Unlimited read access is included in all access profiles used by

Aleris Närsjukvård AB in TakeCare, but not necessarily authorized to

prepare care documentation.

Only those executives who actively participate in the care of a patient

which has an access option to personal data in TakeCare. Every

users at Aleris Närsjukvård AB have individual permissions, including

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 in to 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, as in TakeCare

called a barrier area. An example of a "box" / care unit is Dalengeriatriken. In this case, the user only sees data about

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

information, ie. all care documentation about the patient. This also applies if

the device can be divided into smaller units or teams.

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

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

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

competence beyond that, e.g. if a doctor works all over

area of activity, he is given access to it. Access for

the users within ASIH are limited in such a way that they initially can not

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

patients who are registered there, unless the manager orders one

competence.

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

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

within Aleris Närsjukvård AB, either because there is a 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 that

the employee has an active service at is pre-selected.

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

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

Närsjukvård AB (ie to all different care units within Aleris Närsjukvård AB)

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

concerns the medical certificates to the Swedish Social Insurance Agency. Aleris Närsjukvård AB states that

users are informed that they are not allowed to go into journals and read without

be competent to do so. Aleris Närsjukvård AB believes that it is a shortcoming that

the company within the framework of internal secrecy can not restrict

the reading authority between the operations in Aleris Närsjukvård AB.

The only option available to restrict 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' journal the user of the current care unit

can see, and whether other care providers' users should be able to see the medical record with it

current care unit. Aleris Närsjukvård AB does not use these

protected entities in TakeCare as the company believes this could

involve a patient safety risk.

Coherent record keeping

Aleris Närsjukvård AB has mainly stated the following.

Needs and risk analysis

There is no specific needs and risk analysis produced for cohesion

record keeping.

Authorization of access to personal data about patients

Aleris Närsjukvård AB participates in systems for coherent record keeping through

the TakeCare journal system and the NPÖ journal 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.

Before that, the user must first choose a specific care provider and then

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

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

or an emergency box. By clicking on any of the options get

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

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

and read without being competent to do so.

Users can read it as unlimited through coherent record keeping

written on other caregivers' units, with the patient's consent, with

except if the patient has chosen to block his medical record or if the device is one

so-called protected device.

If the user wants to take care of care documentation from another care provider

the user must document that they have obtained a consent from the patient.

It is not possible to qualify, for a professional group, that one

only takes part in medical records within Aleris Närsjukvård AB.

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

stated that there are opportunities to restrict access in TakeCare states

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

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

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

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

patient safety risk, as the restrictions cannot be lifted

obtained consent from patients or in emergency situations. Aleris

Närsjukvård AB also believes that this would entail 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 are cared for

where often have contact with many caregivers and thus have a great need

of cohesive care.

NPÖ

If a user who has been granted permission wants to use NPÖ can

This is done in two ways. The user can either go directly into NPÖ and

enter an optional social security number which the system then searches for, or so

the user first enters TakeCare and enters the patient's key

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

available about the patient in NPÖ.

Documentation of access (logs)

Aleris Närsjukvård AB has stated the following.

TakeCare

The documentation that is displayed when removing the access logs in TakeCare is;

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

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

the patient during the selected time period, time and date of the most recent

the opening. Regarding which user has opened the journal is indicated

social security number and identification number of the specific unit,
for example ASIH. It is also clear from which device the user has been
inside by specifying the specific department of the current care unit.
In the usual log extracts, it is not clear what actions the user is taking
has taken or how long someone has been in the current journal, 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 is displayed when extracting access logs in NPÖ is;
information about the patient, which user has opened the record, from
which device the user has been in, for example Dalen geriatrics, date
and time of opening and what measures the user has taken.

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

Aleris Närsjukvård AB has in its comments on the letter Final communication
prior to a decision received by the Swedish Data Inspectorate on 16 March 2020 stated among
other the following.

After the Data Inspectorate's inspection, Aleris Närsjukvård AB, together
with certain other actors, initiated and worked with
technical changes and improvements in the opportunities for individuals
eligibility allocations in TakeCare and indirectly in NPÖ. This work has led
for the implementation of new technical solutions at the system supplier such as
has now, in significant respects, rectified the shortcomings of Aleris
Närsjukvård AB as previously caused by the system technical limitations.

Aleris Närsjukvård AB further states that a further review took place

in 2019 by the Swedish Health and Care Inspectorate (IVO). IVO reviewed

compliance with the law on information security for socially important people and

digital services (NIS law). Part of the review concerned

information security including authorization management and

risk work. IVO's decision states, in terms of eligibility allocation

and risk work, the following. “Risk analyzes are also performed for staff,

for example in connection with employee interviews. Background checks are done

on all employees based on three different levels. Great emphasis is placed

authority control. Praktikertjänst N.Ä.R.A. AB decides on each

employees' level of access to the company's information. Removal of

permissions when the employment ends are done automatically via one

authorization system. " Aleris Närsjukvård AB states that it is IVO's final

The decision states that the company complies with the NIS Act in all respects

applicable directive.

Aleris Närsjukvård AB also states that in connection with the introduction of

the data protection ordinance and the NIS law, the company has prioritized routines and

processes in patient safety work at most, followed by ongoing

change work regarding the remaining privacy protection measures. When it

applies to the authorization allocation, it always has, even at

the time of inspection, characterized by the narrowest possible competence, weighed against

current role / assignment in the company and the need for support in operations and

patient safety considerations required for each position and

tasks, taking into account the least possible impact on

information security and privacy. As previously reported

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

the inspection opportunity meant that Aleris Närsjukvård AB could not then introduce

these restrictions in full, which have 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 been made. Among other things, it has previously

the question “What risks would an overly limited allocation of privileges

bring ”has been removed and replaced with the question“ Anything more? ”, 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 25 May 2018 and

is the primary legal regulation in the processing of personal data. This

also applies to health care.

The basic principles for the processing of personal data are set out in

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

security pursuant to Article 5 (1) (f), which states that personal data shall be processed

in a way that ensures appropriate security for personal data,

including protection against unauthorized or unauthorized treatment and against loss;

destruction or damage by accident, using appropriate

technical or organizational measures.

Article 5 (2) states the so-called liability, ie. that it

personal data controllers must be responsible for and be able to show that the basics

the principles set out in paragraph 1 are complied with.

Article 24 deals with the responsibility of the controller. Of Article 24 (1)

it appears that the person responsible for personal data is responsible for implementing appropriate

technical 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.

Article 32 regulates the security of the processing. According to paragraph 1

the personal data controller and the personal data assistant shall take into account

of the latest developments, implementation costs and treatment

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

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

take appropriate technical and organizational measures to ensure a

level of safety appropriate to the risk (…). According to paragraph 2,

when assessing the appropriate level of safety, special consideration is given to the risks

which the treatment 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 in assessing the risk to natural persons

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

personal data covered by professional secrecy, health data or

sexual life, if the processing of personal data concerning vulnerable physical persons takes place

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

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

Furthermore, it follows from recital 76 that the likelihood and seriousness of the risk for it

data subjects' rights and freedoms should be determined on the basis of processing

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

on the basis of an objective assessment, which determines whether

the data processing involves a risk or a high risk.

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

the meaning of the Data Protection Regulation's requirements for security in

Processing of personal data.

The Data Protection Regulation and the relationship with complementary national

provisions

According to Article 5 (1). a of the Data Protection Regulation, the personal data shall

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

legal basis by at least one of the conditions of Article 6 (1) being met.

The provision of health care is one such task of general

interest referred to in Article 6 (1) (e).

In health care, the legal bases can also be legal

obligation under Article 6 (1) (c) and exercise of authority under Article 6 (1) (e)

updated.

When it comes to the legal bases legal obligation, in general

interest or exercise of authority by the Member States, in accordance with Article 6.2, maintain or introduce more specific provisions for adaptation the application of the provisions of the Regulation to national circumstances. National law may lay down specific requirements for the processing of data and other measures to ensure legal and fair treatment. But there is not only one possibility to introduce national rules but also one duty; Article 6 (3) states that the basis for the treatment 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 specific provisions to adapt the application of the provisions of the Data Protection Regulation. Union law or the national law of the Member States law must fulfill an objective of general interest and be proportionate to it legitimate goals pursued.

Article 9 states that the treatment of specific categories of personal data (so-called sensitive personal data) is prohibited. Sensitive personal data includes data on health. Article 9 (2) states except when sensitive personal data may still be processed.

Article 9 (2) (h) states that the processing of sensitive personal data may be repeated the treatment is necessary for reasons related to, among other things the provision of health care on the basis of Union law or national law of the Member States or in accordance with agreements with professionals in the field of health and provided that the conditions and protective measures provided for in

referred to in paragraph 3 are met. Article 9 (3) requires a regulated duty of confidentiality.

This means that both the legal bases of general interest,

exercise of authority and legal obligation in the treatment of the vulnerable

personal data under the exemption in Article 9 (2). h need

supplementary rules.

Supplementary national regulations

In the case of Sweden, both the basis for the treatment and those

special conditions for the processing of personal data in the field of health and

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

the Patient Data Ordinance (2008: 360). I 1 kap. Section 4 of the Patient Data Act states that

the law complements the data protection regulation.

The purpose of the Patient Data Act is to provide information in health and

healthcare must be organized so that it meets patient safety and

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

personal data shall 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 have access to it

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 legislator has

thus through the regulation made a balance in terms of how

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

as the right to privacy in the processing of personal data.

The National Board of Health and Welfare has, with the support of the Patient Data Ordinance, issued regulations and general advice on record keeping and processing of personal data in health care (HSLF-FS 2016: 40). The regulations constitute such supplementary rules, which shall be applied in the care provider's treatment of personal data in health care, see chap. Section 1 of the Patient Data Act.

National provisions that supplement the requirements of the Data Protection Regulation security can be found in Chapters 4 and 6. the Patient Data Act and Chapters 3 and 4 HSLF-FS 2016: 40.

Requirement to make a needs and risk analysis

According to ch. 4, the care provider must § 2 HSLF-FS 2016: 40 make a needs and risk analysis, before the allocation of authorizations in the system takes place.

That both the needs and the risks are required is clear from the preparatory work to the Patient Data Act, prop. 2007/08: 126 pp. 148-149, as follows.

Authorization for staff's electronic access to patient information shall be restricted to what the executive needs to be able to perform his duties in health and healthcare. This includes that authorizations should be followed up and changed or restricted accordingly hand as changes in the tasks of the individual executive give rise to it.

The provision corresponds in principle to section 8 of the Health Care Register Act. The purpose of the provision is to imprint the obligation on the responsible caregiver to make active and individual eligibility assignments based on analyzes of which details are different staff categories and different types of activities need. But it's not just needed needs analyzes. Risk analyzes must also be done where different types of risks are taken into account, such as may be associated with an overly availability of certain types of information.

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

may require special risk assessments.

In general, it can be said that the more comprehensive an information system is, the greater the amount

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

categories of healthcare professionals for electronic access to data in

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

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

allocation of competence should - even if it has points from the point of view of efficiency - be regarded as an unjustified

dissemination of medical records within an

not accepted.

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

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

applies to staff who work with business follow-up, statistics production, central

financial administration and similar activities that are not individual-oriented, it should be

most executives have enough access to information that can only be indirectly derived

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

data that directly point out individual patients should be strong in this area

limited to individuals.

Internal secrecy

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

regulates how privacy protection is to be handled within a care provider's business

and in particular employees' opportunities to prepare for access to

personal data that is electronically available in a healthcare provider

organisation.

It appears from ch. Section 2 of the Patient Data Act, that the care provider shall decide

conditions for granting access to such data

patients who are fully or partially automated. Such authorization shall

limited to what is needed for the individual to be able to fulfill theirs

tasks in health care.

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

users are assigned an individual privilege to access

personal data. The caregiver's decision on the allocation of eligibility shall

preceded by a needs and risk analysis.

Coherent record keeping

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

which means that a care provider - under the conditions specified in § 2 of this

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

caregivers for purposes related to care documentation. The access to

information is provided by a healthcare provider making the information about a patient

which the care provider registers if the patient is available to other care providers

which participates in the cohesive record keeping system (see Bill 2007/08: 126

p. 247).

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

allocation and access control at cohesion

record keeping. The requirement that the care provider must perform a needs and risk analysis

before the allocation of permissions in the system takes place, thus also applies in systems

for coherent record keeping.

Documentation of access (logs)

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

access to such data on patients kept in whole or in part

automatically documented and systematically checked.

According to ch. 4 Section 9 HSLF-FS 2016: 40, the care provider shall be responsible for that

1. the documentation of the access (logs) states which

measures taken with information on a patient,

2. it appears from the logs at which care unit or care process

measures have been taken,

3. the logs indicate the time at which the measures were taken;

4. the identity of the user and the patient is stated in the logs.

The Data Inspectorate's assessment

Responsibility of the data controller for security

As previously described, Article 24 (1) of the Data Protection Regulation provides a

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement is partly to ensure that

the processing of personal data is carried out in accordance with

the Data Protection Ordinance, and that the data controller must be able to

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

the Data Protection Regulation.

The safety associated 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 shall be both technical and

organizational and they must ensure a level of security appropriate in

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 data subjects' rights and freedoms and assess
the probability 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 the significance of what personal data is processed, how many
data, it is a question of how many people process the data, etc.
The health service has a great need for information in its operations. The
It is therefore natural that the possibilities of digitalisation are utilized as much as
possible in healthcare. Since the Patient Data Act was introduced, a lot

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

The data processed must be protected from outside actors as well

the business as against unauthorized access from within the business. It appears

of Article 32 (2) that the data controller, in assessing the appropriate

level of security, in particular to take into account the risks of unintentional or illegal

destruction, loss or for unauthorized disclosure or unauthorized access. In order to

be able to know what is an unauthorized access it must

personal data controllers must be clear about what an authorized access is.

Needs and risk analysis

I 4 kap. Section 2 of 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 and

risk analysis before the allocation of authorizations in the system takes place. This means that

national law prescribes requirements for an appropriate organizational measure that shall:

taken before the allocation of permissions to the journal system takes place.

A needs and risk analysis must include an analysis of the needs and a

analysis of the risks from an integrity perspective that may be associated

with an overly allotment of access to personal data

about patients. Both the needs and the risks must be assessed on the basis of them

tasks that need to be processed in the business, what processes it is

the question of whether and what risks to the privacy of the individual exist.

The assessments of the risks need to be made on the basis of organizational level, there

for example, a certain business part or task may be more

more sensitive to privacy than another, but also based on the individual level, if any

the question of special circumstances that need to be taken into account, such as

that it is a question of protected personal data, publicly known persons or

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

the risk assessment. The preparatory work for the Patient Data Act shows that the more

comprehensive an information system is, the greater the variety

eligibility levels must exist (Bill 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 should

kept up to date.

In summary, the regulation requires that the risk analysis identify

- different categories of data,
- categories of data subjects (eg vulnerable natural persons and children), or
- the scope (eg number of personal data and registered)
- negative consequences for data subjects (eg 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

Processing of personal data. This applies to both internal secrecy

as in coherent record keeping.

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

based on whether there is protected personal data that is

classified, information on public figures, information from

certain clinics or medical specialties (Bill 2007/08: 126 p. 148149).

The risk analysis must also include an assessment of how probable and serious

the risk to the data subjects' rights and freedoms is based on

the nature, scope, context and purpose of the treatment (recital 76).

It is thus through the needs and risk analysis that it

personal data controller finds out who needs access, which

information the accessibility shall include, at what times and at what

context access is needed, while analyzing the risks to it

the freedoms and rights of the individual that the treatment may lead to. The result should

then lead to the technical and organizational measures needed to

ensure that no access other than that of need and

the risk analysis shows that it is justified to be able to do so.

When a needs and risk analysis is missing prior to the allocation of eligibility in

system, lacks the basis for the personal data controller on a legal

be able to assign their users a correct authorization. The

the data controller is responsible for, and shall have control over, the

personal data processing that takes place within the framework of the business. To

assign users one upon access to journal system, without this being founded

on a performed needs and risk analysis, means that the person responsible for personal data

does not have sufficient control over the personal data processing that takes place in

the journal system and also can not show that he has the control that

required.

When the Data Inspectorate has requested a documented needs and
risk analysis, Aleris Närsjukvård AB has referred to the document Allocation of
competencies, needs and risk analysis, template: Functional descriptions and
mission. The document states that the responsible manager must perform a needs and
risk analysis when hiring an employee based on the employee's needs for
authorizations for access to 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 a question - “What risks would
an overly limited allocation of privileges? ” Before the allocation of
an authorization profile states that risks and needs must be weighed. The
The privacy risk addressed in the document also consists of a question - “Which
risks regarding patient integrity, does this mean that the authorization is granted? ” The
the only suggestion of risk given is “risk of access to, at the time of care, no
necessary patient information in TakeCare through the ability to
coherent record keeping ”.

As stated above, in a needs and risk analysis, both the needs and
the risks are assessed on the basis of the data that need to be processed in
the business, what processes are involved and what are the risks for it
individual integrity that exists on both organizational and individual
level. It is thus a question of a strategic analysis at a strategic level, which
shall provide an authorization structure that is adapted to the activities. It should
result in authorization assignments but it is not
the instructions to the person who assigns the permissions that are the analysis.

During the Data Inspectorate's inspection, Aleris Närsjukvård AB was unable to do so

present a needs and risk analysis - either within the framework of the internal

confidentiality or within the framework of coherent record keeping. Aleris

Närsjukvård AB's document lacks the basic inventory of

users' need for access and risk analysis, nor has it

made a balance between needs and the actual privacy risks that

the processing of personal data gives rise to.

In its analysis, Aleris Närsjukvård AB has not taken into account negative consequences for

registered, different categories of data, categories of registered, or

the extent of the number of personal data and data subjects affects the risk of

rights and freedoms of natural persons by Aleris Närsjukvård AB's

processing of personal data in TakeCare and NPÖ. It is also missing

special risk assessments based on whether there are e.g. protected

personal data that is classified, confidential information

persons, information from certain clinics or medical specialties

or other factors that require special protective measures. It is also missing

assessment of the probable and serious risk to those registered

rights and freedoms are judged to be.

In summary, the Data Inspectorate finds that the documents

Allocation of authorizations, needs and risk analysis, template:

Functional descriptions and assignments, Assessment of access rights

to patient data and to other systems and

Authorization roles / profiles in patient data systems, which have been reported by Aleris

Närsjukvård AB does not meet the requirements for a need and

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

carried out a needs and risk analysis within the meaning of ch. § 2

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

the framework for the unified record keeping, according to chapters 4 and 6, respectively.

the Patient Data Act. This means that Aleris Närsjukvård AB has not taken

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 personal data has a security that is appropriate in

in relation to the risks.

Authorization of access to personal data about patients

As reported above, a caregiver may have a legitimate interest in having

a comprehensive processing of data on the health of individuals. Notwithstanding this shall

access to personal data about patients may be limited to

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

With regard to the allocation of authorization for electronic access according to ch.

§ 2 and ch. 6 Section 7 of the Patient Data Act states in the preparatory work, Bill.

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

the journal system and that the permissions should be limited to what the user

need to provide the patient with good and safe care. It also appears that “a

more extensive or coarse-grained eligibility should be considered as one

unauthorized dissemination of journal information within a business and should as

such is not accepted. "

In health care, it is the person who needs the information 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 person responsible for personal data finds out who
who need access, what information the access should include, at which
times and in which contexts access is needed, and at the same time
analyzes the risks to the individual's freedoms and rights
the treatment can lead to. The result should then lead to the technical and
organizational measures needed to ensure no allocation
of eligibility provides further access opportunities than the one that needs and
the risk analysis shows is justified. An important organizational measure is to provide
instruction to those who have the authority to assign permissions on how this
should go to and what should be considered so that it, with the needs and risk analysis
as a basis, becomes a correct authorization allocation in each individual case.
According to Aleris Närsjukvård AB, there is an opportunity to limit users
access to patients' data, within the framework of internal confidentiality, i
TakeCare through the so-called protected devices. Aleris Närsjukvård AB
has not, however, introduced such devices. The only restriction on access that
are in the system concerning the medical certificates to the Swedish Social Insurance Agency, which are not all
users have access to.
Aleris Närsjukvård AB has expressed it as the permissions in the interior
secrecy 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, ie. all care documentation about the patient. This also applies if

the device can be divided into smaller units or teams. Within the framework of it
internal privacy, the user can himself by active selections tick boxes such as
provides access to care documentation at all care units within Aleris
Närsjukvård AB, either because there is a consent from the patient
or that it is an emergency.

When it comes to access to data within a caregiver's business, so
it follows from ch. 4 § 4 HSLF-FS 2016: 40 that the care provider “shall be responsible for that
information on which other care units or in which other care processes
there is information about a particular patient can not 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 information then does not get
be made available without the authorized user making another active
choice."

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

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

that the individual should be able to fulfill his tasks in health and

healthcare, ie. only those who need the information should be able to have

access to them.

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

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

there are opportunities for the caregiver to restrict the user's access to

personal data of other care providers.

With regard to access to personal data about patients within its framework

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

Närsjukvård AB has been granted authorization. The Data Inspectorate can state that

a limit has been placed on the number of users, based on the 1,700

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

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

not that there has been any restriction on what documentation these

users can take part in NPÖ.

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

and enter an optional social security number which the system then searches for,

or the user first enters TakeCare and enters the patient's key

social security number and then make an exit to the information that is available

about the patient in NPÖ.

Because different users have different tasks within different

work areas, users' access to the journal 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 medical record 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 processed
within the framework of NPÖ.
That the allocation 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 identified which access is justified for
users based on such an analysis. Aleris Närsjukvård AB thus does not have
have taken appropriate measures, in accordance with Article 32
the Data Protection Regulation, to restrict users' access to
patients' personal data in the medical record system. This in turn has meant
that there has been a risk of unauthorized access and unauthorized distribution of
personal data partly within the framework of internal secrecy, partly within the framework
for the unified record keeping.
In light of the above, the Swedish Data Inspectorate can state that Aleris
Närsjukvård AB has processed personal data in violation of the article
5.1 f and Article 32 (1) and (2) of the Data Protection Regulation by Aleris
Närsjukvård AB has not restricted users' permissions for access to
the journal system TakeCare and NPÖ to what is only needed to
the user must be able to fulfill his tasks in health and

healthcare according to ch. 4 § 2 and ch. 6 Section 7 of the Patient Data Act and Chapter 4 § 2 HSLF-FS 2016: 40. This means that Aleris Närsjukvård AB has not taken measures to ensure and, in accordance with Article 5 (2) (i) the Data Protection Regulation, be able to demonstrate appropriate security for personal data.

Documentation of access (logs)

The Data Inspectorate can state that of the logs in TakeCare and NPÖ information about the specific patient, which user has opened the journal, measures that have been 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.

The Data Inspectorate 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. 9 § HSLF-FS 2016: 40 and has thus taken the appropriate technical measures in accordance with Article 32 of the Data Protection Regulation.

Opinion on the Data Inspectorate's letter Final communication after decision

Aleris Närsjukvård AB has supplemented its previous tasks with one opinion received by the Data Inspectorate on 16 March 2020, where Aleris Närsjukvård AB states that it has conducted work with technical changes and improvements in the opportunities for individuals

eligibility allocations in TakeCare and indirectly in NPÖ. The work has led to implementation of new technical solutions at the system supplier such as has now, in significant respects, rectified the shortcomings of Aleris Närsjukvård AB as previously caused by the system's technical limitations.

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

The Data Inspectorate considers it positive that Aleris Närsjukvård AB has contributed to the implementation of new technologies solutions in TakeCare, which has corrected shortcomings at Aleris Närsjukvård AB. However, it is not clear what these shortcomings are or in what way the shortcomings has been corrected within the framework of Aleris Närsjukvård AB's award of permissions.

The Data Inspectorate 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 current Directive, and not on the basis of the Data Protection Regulation and the provisions of the Patient Data Act. The NIS law aims to achieve a high level on the security of networks and information systems for socially important people services while the data protection rules aim to protect them freedoms and rights were registered in the processing of personal data.

Choice of intervention

Legal regulation

If there has been a violation of the Data Protection Regulation

The Data Inspectorate a number of corrective powers available under the article

58.2 a - j of the Data Protection Regulation. The supervisory authority can, among other things

instruct the person responsible for personal data to ensure that the processing takes place in

in accordance with the Regulation and if required in a specific way and within a

specific period.

It follows from Article 58 (2) of the Data Protection Ordinance that the Data Inspectorate in

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

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

the circumstances of each individual case.

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. Of central importance for the assessment of

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

in the case of a minor infringement, the supervisory authority may, according to reasons

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

penalty fee.

Order

As mentioned, the health service has a great need for information in its

Operation. It is therefore natural that the possibilities of digitalisation

be utilized as much as possible in healthcare. Then the Patient Data Act

was introduced, a very extensive digitalisation has taken place in healthcare. As well

the data collections size as how many people share information with

each other has increased significantly. At the same time, this increase means that the requirements

increases on the personal data controller, because the assessment what is a

appropriate safety is affected by the scope of treatment.

In health care, this means a great responsibility for it

personal data controller to protect the data from unauthorized access,

among other things by having an authorization allocation that is even more

comminuted. It is therefore essential that there is a real analysis of the needs

based on different activities and different executives. Equally important is that

there is an actual analysis of the risks from an integrity perspective

may occur in the event of an override of access rights. From

this analysis must then be restricted to the individual executive.

This authority must then be followed up and changed or restricted accordingly

hand that changes in the individual executive's duties

reason for it.

The Data Inspectorate's inspection has shown that Aleris Närsjukvård AB has not taken action

appropriate security measures to protect the personal data of 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 do not meet the requirements in Article 5 (1) f

and Article 32 (1) and (2) of the Data Protection Regulation. The omission

includes both the internal secrecy according to ch. the Patient Data Act as it

coherent record keeping according to ch. 6 the Patient Data Act.

The Data Inspectorate therefore submits, pursuant to Article 58 (2) (d) i

the Data Protection Ordinance, Aleris Närsjukvård AB to implement and

document the required needs and risk analysis for the journal systems

TakeCare and NPÖ within the framework of both internal secrecy and within the framework for the unified record keeping. Aleris Närsjukvård AB shall further, on the basis of the needs and risk analysis, assign each user individual access to personal data restricted to only what is needed for the individual to be able to fulfill his tasks in health care.

Penalty fee

The Data Inspectorate can state that the violations basically concern Aleris Närsjukvård AB's obligation to take appropriate safety measures to provide protection of personal data in accordance with the Data Protection Regulation.

In this case, it is a matter of large collections of data with sensitive personal data and extensive powers. The caregiver needs to be involved necessity to have a comprehensive processing of data on the health of individuals. However, it must not be unrestricted but should be based on what individual employees need to be able to perform their tasks. The Data Inspectorate notes that this is information that includes direct identification by the individual through name, contact information and social security number, health information, but it may also be other private information about, for example, family relationships, sexual life and lifestyle. The patient is dependent on receiving care and is thus in a vulnerable situation. The data nature, scope and patients' dependence give caregivers a special responsibility to ensure patients' right to adequate protection for their

personal data.

Additional aggravating circumstances are the treatment of

personal data about patients in the main medical record system belongs to the core of a

the activities of caregivers, that the treatment covers many patients and

the possibility of access refers to a large proportion of the employees. Within the framework of

internal secrecy, 1,700 people have access to relevant information

about 55,000 patients, apart from the information relating to medical certificates

Försäkringskassan, which not all users have access to. In addition

the possibility for the 1,700 persons to access the personal data within

the framework for the unified 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 person responsible for personal data to take measures

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

the assessment of the appropriate level of safety, special consideration shall be given to those risks

which the treatment 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,

pursuant to Article 32 (2) of the Data Protection Regulation. The requirements for health and

the healthcare area, regarding current security measures, has been specified in

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

The Patient Data Act clearly states that requirements are placed on both strategic analysis and

that eligibility is assigned individually and adapted to the current one

the situation. That Aleris Närsjukvård AB has granted authorizations without

following these requirements means that the action was taken intentionally and is thus assessed

as more serious.

In determining the seriousness of the infringements, it can also be stated that the infringements also cover the basic principles set out in Article 5 (i) the Data Protection Regulation, which is one of the more serious infringements that can provide a higher penalty fee under Article 83 (5) of the Data Protection Regulation. Taken together, these factors mean that the infringements are not to be assessed as minor violations without violations that should lead to a administrative penalty fee.

The Data Inspectorate considers that these violations are closely related to each other. That assessment is based on the need and risk analysis form the basis for the allocation of the authorizations. The Data Inspectorate therefore considers that these infringements are so closely linked that they constitute interconnected data processing within the meaning of Article 83 (3) (i) the Data Protection Regulation. The Data Inspectorate therefore decides on a joint penalty fee for these infringements.

According to Article 83 (3), the administrative penalty fee may not exceed the amount of the most serious infringement in the case of one or the same data processing or interconnected data processing.

The administrative penalty fee shall be effective, proportionate and deterrent. This means that the amount must be determined so that it the administrative penalty fee leads to correction, that it provides a preventive effect and that it is also proportional in relation to both current violations as to the ability of the supervised entity to pay.

For the purposes of calculating the amount, see Article 83 (5) (i)

Data Protection Regulation that companies committing infringements such as the current ones

Sanctions of up to EUR 20 million or four may be imposed

percent of total global annual sales in the previous financial year,

depending on which value is highest.

The term company includes all companies that conduct a financial

activity, regardless of the legal status of the entity or the way in which it operates

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

infringement of the Data Protection Regulation by one of its companies.

Recital 150 in the Data Protection Ordinance states, among other things

following. […] If the administrative penalty fees are imposed on a company,

an undertaking for that purpose should be considered as an undertaking 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 unit. A parent company and a subsidiary are considered

as part of the same economic entity when the parent company exercises one

decisive influence over the subsidiary. The Data Inspectorate therefore adds

as a starting point, the turnover for Aleris Group AB as a basis for

the calculation of the size of the penalty fee.

Aleris Group AB was formed at the end of 2019. Some turnover figures for the whole 2019 is thus not available. There is therefore no information on the annual turnover for determining the amount 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. Recalculated for an entire year, this 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 acquired and since 1 April 2020 has Aleris Group AB as Group parent, it is likely that it actual annual sales for Aleris Group AB this year will be significantly higher.

In the current case, the Data Inspectorate 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 the full year, ie approximately 4.9 billion. The maximum penalty amount that can be determined in the current case is EUR 20,000,000, which is just over four percent of the company's estimated revenue.

In view of the seriousness of the infringements and that the administrative the penalty fee must be effective, proportionate and dissuasive

The Data Inspectorate determines the administrative sanction fee for Aleris Närsjukvård AB to SEK 12,000,000 (twelve million).

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

presentation by the IT security specialist Magnus Bergström. At the final

The case is also handled by the General Counsel Hans-Olof Lindblom, the unit managers

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 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 you received the decision. 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.