Decision

Diarienr

2020-12-02

DI-2019-3846

The board of Capio St. Göran's Hospital

AB

S: t Göransgatan 141

112 81 Stockholm

Supervision under the Data Protection Regulation and

Patient Data Act - needs and risk analysis and

questions about access in journal systems

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

The Data Inspectorate's decision

During a review on April 3, 2019, the Data Inspectorate has found that Capio

S: t Görans Sjukhus AB processes personal data in violation of Article 5 (1) (f) and

5.2, and Article 32 (1) and (2) of the Data Protection Regulation1 by:

1.

Capio S: t Görans Sjukhus AB has not implemented needs and

risk analyzes before the allocation of authorizations takes place in the journal systems

Cambio Cosmic, National Patient Overview and TakeCare accordingly

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

Section 2 The National Board of Health and Welfare's regulations and general guidelines (HSLF-FS 2016: 40)

on record keeping and processing of personal data in health and

healthcare. This means that Capio S: t Görans Sjukhus AB does not have

have taken appropriate organizational measures to ensure

and be able to show that the processing of personal data has one

security appropriate to the risks.

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

for 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).

1

2. Capio S: t Görans Sjukhus AB has not restricted users

privileges for accessing the Cambio Cosmic journal systems,

National patient overview and TakeCare for that alone

needed for the user to be able to fulfill theirs

duties in health care in accordance with 4

Cape. § 2 and ch. 6 Section 7 of the Patient Data Act and Chapter 4 § 2 HSLF-FS

2016: 40. This means that Capio S: t Görans Sjukhus AB does not have

taken measures to be able to ensure and be able to show one

appropriate security for personal data.

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

the Data Protection Ordinance that Capio S: t Görans Sjukhus AB for

infringements 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

30,000,000 (thirty million) kronor.

The Data Inspectorate submits on the basis of Article 58 (2) (d)

the data protection ordinance Capio S: t Görans Sjukhus AB to implement and

document the required needs and risk analyzes for the medical record systems

Cambio Cosmic, National Patient Overview and TakeCare and that thereafter,

based on these needs and risk analyzes, assign each user

individual access to personal data restricted to

only what is needed for the individual to be able to fulfill his

duties in health care, in accordance with Article 5 (1) (f) and

Article 32 (1) and (2) of the Data Protection Ordinance, Chapter 4 § 2 and ch. 6 § 7

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 April 3, 2019 reviewed Capio S: t Görans Sjukhus AB in question their decision on the allocation of competences has been preceded by a need and risk analysis. The supervision has also included how Capio S: t Görans has allocated permissions for accessing the Cambio Cosmic master record system (below) Cosmic) and the journal systems National Patient Overview (hereinafter NPÖ) and TakeCare and what access possibilities the assigned permissions provide within the framework of the internal secrecy according to ch. Patient Data Act, as the cohesive record keeping according to ch. the Patient Data Act.

In addition to this, the Data Inspectorate has also examined the documentation of access (logs) that are in the journal systems.

The Data Inspectorate has only examined users' access 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 system (eg issuing prescriptions, writing referrals, etc.).

Due to what has emerged about Capio St. Göran's opinion in issue of restricting the readability of its TakeCare users, Capio St. Göran was asked to comment in particular on what had emerged in one opinion from Karolinska University Hospital, which also uses TakeCare, where the technical possibilities regarding TakeCare were described.

What has emerged in the case

Capio St. Göran has mainly stated the following.

The responsibility for personal data

Capio S: t Görans is the care provider and person responsible for personal data.

The business

Capio S: t Görans is a limited company that runs an emergency hospital according to a care agreement with the Stockholm Region. Capio S: t Görans has 3,084 ongoing employees.

In addition to this, there are 340 contractors, e.g. rental staff and students.

Capio S: t Görans is part of the Capio Group, which was acquired in November 2018 of and now part of the French group Ramsay Générale de Santé S.A.

Capio S: t Görans claims that according to the agreement signed by Capio Group with the Stockholm Region, regarding the operation of St. Göran's Hospital, the company shall Capio St. Göran's Hospital is managed as a completely independent business, separate from Capio Group / Ramsay Générale de Santé, why sales for Capio Group and Ramsay Générale de Santé do not apply to Capio S: t Görans Hospital.

Journal system

Capio St. Göran's has been using Cosmic as its main journal system since 2005 within the framework of internal secrecy and for coherent record keeping within the Capio Group. In addition to this, Capio uses St. Göran's NPÖ and TakeCare for cohesive record keeping.

In the journal system Cosmic, there is personal information about 492,264 unique patients. Cosmic has 2,764 active users. Capio St. Göran's is part of the TakeCare medical record system together with a large number of other care providers. IN TakeCare has data on approximately 3 million unique patients registered. There are 606 people at Capio S: t Görans who have access to

the TakeCare journal system.

Internal secrecy

Needs and risk analysis

Capio St. Göran has mainly stated the following.

Capio S: t Görans has stated that they have previously carried out a needs and

risk analysis. However, it is not preserved. In light of this need and

risk analysis, Capio St. Göran developed guidelines for authorization allocation, which

is used by the business managers when allocating authorizations.

In connection with the inspection on April 3, 2019, Capio S: t Görans stated

that they had not decided when a needs and risk analysis should be made, but

if a new event occurs - e.g. if a new clinic is opened - then it is done

a new needs and risk analysis. On March 19, 2020, Capio St. Göran joined

a document entitled “Needs and risk analysis, eligibility profiles in Cosmic

Clinical staff ”, dated 14 January 2020.

Authorization of access to personal data about patients

Capio St. Göran has mainly stated the following.

Capio S: t Görans is divided into clinics and it is the business managers at

each clinic, which is responsible for assessing which qualifications should

assigned to each employee. Capio S: t Görans demands that the care staff

complies with the Patient Data Act when accessing patient data. Capio St. Göran's has

eligibility guidelines developed according to a needs and

risk analysis for eligibility allocation according to established profiles in Cosmic.

Capio S: t Görans sees its operations as an "emergency basic emergency mission", which

means the influx of patients and the tasks to be performed
mainly comes from the emergency room. To the emergency flow and
the emergency hospital assignment must be able to be carried out, broad allocations of are needed
permissions. Capio St. Göran emphasizes that they have an extensive
operations in emergency care, with approximately 100,000 emergency visits per year. This
means that there is a very low proportion of pre-planned care at the hospital.
These guidelines state that they are hospital-wide and form the framework for it
responsibility, regarding the allocation of access and authority for journal information. IN
the guidelines state that the term competence refers to the technical
the opportunity to take part in information, ie. what an employee can do, not
what the employee may do in an individual case. The guidelines state that Capio
St. Göran has made the assessment that within the internal secrecy has as
rule all employees in patient-centered work at the hospital's clinics one
general need for access and thus access to these devices
collective documentation. Access to information outside the respective
business area requires active choices in the system. Patients with increased need
of privacy protection has the opportunity for confidentiality even between the traditional ones
clinics by requesting a block. However, this barrier is possible to break.
However, according to the guidelines, a barrier may not be placed between clinics that
together participate in a joint care process, or on such information
which must be available in all care processes at the hospital.
The guidelines state that the term permitted access refers to the question of when
it is allowed to take part in journal information, which is mainly due to
the employee's needs in the individual case and the guidelines state a number
examples of situations where access is allowed. The guidelines thus contain
instructions that limit what employees may do within that space

for access that they have been granted in accordance with the above paragraph, ie. the space that is technically possible within the "competence". According to these instructions, it is required that an employee participates in the care of a patient for that it should be permitted to access personal data about him. Beyond this access is permitted for systematic quality work on behalf of operations manager.

Capio S: t Görans has also developed routines for allocating authorization. Of these are essentially identical assessments regarding the interior

secrecy. The assessment is that the need to be able to assimilate clinical information about each patient is crucial to be able to conduct a healthcare with good quality and patient safety. Based on this has that rule all employees with clinical assignments access to Cosmics key features. Access to information outside the respective business area requires active choices in the system. The risk of employees improperly have access to patient data is reduced by configuration that requires active choices as well as regular and systematic log monitoring.

The heads of operations have the opportunity to receive support from the chief physician, data protection officer and the hospital's chief medical information officer at this assessment. Authorization administrators at Capio S: t Görans have a large experience of the competency structure. They do role checking and ordered profile before granting authorizations.

In Cosmic, there are ready-made roles for different categories of employees, e.g. doctor and nurse. In addition, there are ready-made profiles for other roles

such as nursing students or medical graduates. Capio S: t Görans
emphasizes that the employees who participate in work close to the patient have one
general need for all documentation at the hospital's clinics.
Employees can read all information in Cosmic. There are none
restrictions on access possibilities in the authorizations provided by Capio S: t Görans
assigns employees.

Active choices

Capio St. Göran has stated that Cosmic is configured in such a way that
employees first and foremost get to see what they need for their job. This
means, among other things, that Cosmic initially displays information attributable to it
clinic where the employee in question is active, the so-called "home clinic".
However, employees have the opportunity to take part in tasks through "active choices"
concerning patients at other clinics. This means that information about on
which other care units or in which other care processes there is information
if a particular patient is not made available without that user having made one
a position on whether he or she has the right to take part in it
information. After an active selection, the user can click on to all
information available about the patient within the framework of internal confidentiality
at Capio S: t Görans, where the user can, among other things, take part in one
"Total record" for the patient. Then the employee sees all the information about
the patient, apart from the information that has been blocked.

Coherent record keeping

Capio St. Göran has mainly stated the following.

Needs and risk analysis

Capio S: t Görans has stated that they have previously carried out a needs and risk analysis. However, it is not preserved. In light of this need and risk analysis, Capio St. Göran developed guidelines for authorization allocation, which is used by the business managers when allocating authorizations.

On March 19, 2020, Capio St. Göran submitted two documents named “Needs and risk analysis, eligibility profiles in NPÖ” and “Needs and risk risk analysis, readability in TakeCare ”. These documents are dated the 17th January 2020.

Authorization of access to personal data about patients

Capio S: t Görans has stated the following about the authorization allocation within the framework for the unified record keeping.

Capio S: t Görans requires that the care staff comply with the Patient Data Act access to patient data, all access is logged and access is followed up through log checks.

Capio St. Göran's Hospital acts as a personal data assistant for the others the healthcare providers within the Capio Group that use Cosmic and personal data assistant agreements are established regarding the provision of operational and management-related services. Employee at Capio S: t Görans can access patient data related to the attention signal (UMS) for other companies within the Capio Group. The attention signal shows information on warnings (medicines, foods), observances, infections and treatment / condition that needs attention (ex: dialysis). Individual patients' contact overview can be displayed for users with special selections indicates two different settings. Then the date and time of the care contact is displayed, Medically responsible and caring unit and the status of the care contact.

When it comes to the other journal systems, the normal time is that

the staff first uses Cosmic and then NPÖ. If

the information is missing in NPÖ, the use of TakeCare may be considered. The

is a deliberate action on the part of the staff when they take part in information in

TakeCare.

A prerequisite for being able to take part in information in NPÖ or TakeCare is that

the employee is logged in to Cosmic and works with a specific patient. When

the employee then activates and logs in to NPÖ or TakeCare,

the personal patient's social security number will be transferred to NPÖ or

TakeCare and thereby control access to data in such a way that

the employee can take part in information concerning the patient in question.

The above-mentioned guidelines for authorization allocation state, among other things

the following in the case of coherent record keeping. Permissions, ie. technical

opportunity to take part in information in coherent record keeping, must be controlled

according to the employees' need to be able to perform their work in the same way as

for local journals. Eligibility should be offered to all physicians in clinical service

as well as other key staff such as coordinators and administrative staff

who need access to this type of information in order to prevent, investigate,

treat or plan for patients in the care chain. To access

a coherent medical record must be permitted, the active consent of the patient is required.

The precondition for obtaining consent is that there is an ongoing,

planned or completed care relationship and that collection of the data

contributes to the patient's health.

Capio S: t Görans states that they have been the subject of the Inspectorate for care and

care (IVO) supervision according to the Patient Safety Act, which concerned the examination of

how Capio St. Göran ensures that patients receive the right medicine

enrollment in a ward and discharge to another clinic. This

inspection ended without criticism after Capio St. Göran has already described

measures taken and planned which were intended, among other things, to ensure

access to drug information and medical records in others

caregivers, mainly through TakeCare and NPÖ. Capio St. Göran emphasizes

that IVO highlighted the importance of employees with care assignments having enough

extensive eligibility for NPÖ and TakeCare and what risks would

be able to arise for patient safety if physicians and coordinators

nurses would not have sufficiently broad qualifications.

NPÖ

In NPÖ, doctors and nurses in particular can take part in all of them

made available information concerning the patient. If there are additional

categories of people with employee assignments can also be given access.

There is no possibility for the employee to apply freely in NPÖ.

TakeCare

Eligibility for TakeCare is usually assigned to doctors and other professional roles

which has a special task to coordinate care between Capio St. Göran's and

other care providers within the Stockholm Region.

TakeCare uses the "CapioRead" function. It's a finished one

authorization profile and there is no possibility to choose someone else

authorization profile, regardless of the title of the employee. The authority
means only a reading license in TakeCare and it is mainly doctors who
assigned to this as needed, but there may also be needs in others
people. All employees who are active in the emergency department and they
people who participate in the patient's later emergency flow have, for example
read access in TakeCare. These people have access to all the information in
TakeCare. However, this presupposes that the employee clicks on the journal filter in
TakeCare, which means that it is possible to share information with others
healthcare providers. Capio S: t Görans has access in the form of reading rights, through
first choice, for information belonging to Karolinska Hospital and SLSO
within the Stockholm Region.
Capio St. Göran emphasizes that they are Sweden's largest emergency department, calculated
in patients per day. As the care within the Stockholm Region does not use
the same main record system is used NPÖ for coherent record keeping.
However, NPÖ lacks a number of types of information, in particular
information on prescribed and administered drugs, why Capio St.
Göran in recent years also uses TakeCare which is used by others
caregivers in the region. Analyzes of patient safety issues pointed out the shortcoming
on access to drug information as a negative factor. Access to
coherent record keeping is always preceded by a consent, whenever possible
collected, and documented in the patient record.
Capio S: t Görans further states that the reading rights in TakeCare have a filter
which primarily allows reading of information that has arisen within Stockholm
county healthcare area or Karolinska Hospital. The choice of caregiver
is based on decisions about patient flows in the region's overall plan. In and
with Capio St. Göran's being an emergency hospital, it is not possible to know in advance which ones

amounts of information needed in the individual case, but only that

the information supply must be good to ensure a good and

patient-safe care. This means that the read access to systems for

coherent record keeping must be broad. Based on this do

the employee active choices according to the Patient Data Act to take advantage of it

information needed to best care for a patient.

To access TakeCare, you must be logged in to Cosmic on a specific

patient, but it is possible to clear the list and view patient data for one

another social security number. All access is logged and access is followed up through

log checks.

Documentation of access (logs)

Capio St. Göran has mainly stated the following.

In Cosmic, the logs contain several categories of information, including

log date, log hospital, patient's social security number, log social security number,

patient table, patient's name, gender, confidentiality, daily part (day, evening or night),

log clinic, log unit, log user ID (name of the person, title and profession),

module, what activity was performed, log arguments (amount of information),

timestamp and date.

In TakeCare, the logs contain the categories time and date (when any

has been inside), name of the person who has been inside and the patient's

social security number.

At the time of the inspection on April 3, 2019, the Data Inspectorate requested that Capio

St. Göran's supplemented the case with printed logs for Cosmic, NPÖ

and TakeCare.

When the Data Inspectorate received the printed logs for each

journal system, the inspectorate was able to establish that with regard to the log extract

for TakeCare, it was not clear at which care unit or care process

measures have been taken. The Data Inspectorate requested that in addition

information from Capio St. Göran get information on whether this information is

available otherwise.

In an opinion on 19 March 2020, Capio St. Göran stated that there are two

types of log extracts for TakeCare, simple and in-depth, respectively, and that in

both forms of log extracts are reported in the care unit. Capio St. Göran's attached

log extracts to prove this. Of the in-depth log extract for TakeCare

it is clear at which care unit the measures were taken.

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, provided that at least one of the conditions of Article 6 (1) is 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; legal

obligation 6.1. c and the exercise of authority 6.1. e is 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.

Of ch. Section 2 of the Patient Data Act states that the purpose of the Patient Data Act is to

information management in health care must be organized in this way

that it meets patient safety and good quality and promotes

cost-effectiveness. Furthermore, personal data must be designed and otherwise

treated so that the privacy of patients and other data subjects is respected.

In addition, documented personal data must be handled and stored so that

unauthorized persons do not have access to them.

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 patient safety and

privacy requirements.

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 do 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

competency allocation should - even if it has points from an efficiency point of view -

is considered an unjustified dissemination of journal information within a business and should as such

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 employees' opportunities to prepare electronically and automatically

access to personal data that is electronically available in a

caregivers' organization (see Bill 2007/08: 126 p. 141 and p. 239).

It appears from ch. Section 2 of the Patient Data Act stipulates that the care provider must 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 the same

chapter of that law - may have direct access to personal data that is processed

by other care providers 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 also 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 be processed by very

many people. 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

In 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. (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 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 there is no access other than that which is needed and
the risk analysis shows is justified.
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.
At the time of the inspection on April 3, 2019, the Data Inspectorate requested one
documented needs and risk analysis. Capio St. Göran stated that they
has previously carried out a needs and risk analysis, but that it has not
was preserved. Capio St. Göran stated that in the light of this
needs and risk analysis had developed guidelines for authorization allocation,
to be used by the heads of operations at each clinic when they
decides on the allocation of authorizations. Capio S: t Görans has also produced
procedures for allocating authorization. Capio St. Göran has on March 19 given

submit new documents that are stated to be needs and risk analyzes concerning the three current journal systems Cosmic, NPÖ and TakeCare.

The Data Inspectorate has described above the requirements that apply during implementation of a needs and risk analysis. In such a case, both the needs and the risks must assessed on the basis of the information that needs to be processed in the business, which processes it is a question of and what risks to the privacy of the individual available both at the organizational and at the individual level. It is thus the question of a strategic analysis at the strategic level, which should provide one authorization structure that is adapted to the activities.

The Data Inspectorate can state that neither the guidelines for allocation of eligibility, the procedures for granting eligibility or any of the three new ones the documents that are stated to be needs and risk analyzes contain any assessment in terms of the needs of different executives and different kind of activities need. A basic prerequisite for a care providers must be able to meet the requirement to limit the electronic access to personal data about patients to what respectively executives need to be able to perform their duties within health care is that the care provider conducts a needs and risk analysis. There is also no analysis where Capio St. Göran considers the negative consequences for data subjects, different categories of data, categories of registered and to what extent the extent of the number personal data and data subjects affect the risk to natural persons rights and freedoms as a result of Capio St. Göran's treatment of

personal data in Cosmic, NPÖ and TakeCare. There are also no specials

risk assessments based on whether there are e.g. protected personal information

which are classified, information about publicly known persons, information

from certain clinics or medical specialties or other factors

requiring special protection measures. There is also no assessment of how

probable and serious risk to the data subjects' rights and freedoms

is considered to be.

The Data Inspectorate can state that the guidelines for allocation of

eligibility, the procedures for granting eligibility and the three new ones

the documents that are stated to be needs and risk analyzes lack one

basic inventory of users' access and analysis needs

risks, nor has any assessment been made by users

actual needs in relation to the privacy risks that

the processing of personal data gives rise to.

In summary, the Data Inspectorate can state that neither

the guidelines for allocating authorization, the procedures for allocating

authorization or one of the three new documents that are stated to be new needs and risk analyzes meet the requirements for

a needs and risk analysis

and that Capio S: t Görans has not been able to show that they have carried out a needs and risk analysis within the meaning

of ch. 2 § HSLF-FS 2016: 40, whether

within the framework of internal secrecy or within the framework of it

coherent record keeping, according to chapters 4 and 6, respectively. the Patient Data Act.

This means that Capio S: t Görans has not taken appropriate organizational measures

measures in accordance with Article 5 (1) (f) and Article 31 (1) and (2) in order to:

ensure and, in accordance with Article 5 (2), be able to demonstrate that the treatment of

the personal data has a security that is appropriate 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. This is happening

particularly applicable in emergency care. Notwithstanding this, accessibility should

to personal data about patients be limited to what is needed to

the individual must be able to fulfill his tasks.

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.
Capio St. Göran emphasizes that their business is an emergency hospital. They do
that broad allocations of competencies are needed as a result
is a very low proportion of pre-planned care at the hospital.

The Data Inspectorate does not question that employees at Capio S: t Görans
need extensive access to patients' personal data for
to be able to fulfill their duties in health care. This
does not mean, however, that it is permissible to without prior needs and
risk analysis assign all employees with clinical assignments such
included access capabilities. Capio St. Göran's is subject to an obligation
that, having carried out needs and risk analyzes within the meaning referred to in
Chapter 4 § 2 HSLF-FS 2016: 40, assign each employee an individual
competence that is limited to what he needs to be able to fulfill
their duties in health care.
With regard to internal confidentiality, it appears that more than 2,700 employees
at Capio St. Göran's uses Cosmic, which contains information about approx
490,000 unique patients. It has emerged that Capio S: t Görans does not have
restricted users' access to personal data within
the framework for the internal confidentiality of the journal system Cosmic.

Capio St. Göran has stated that the powers within the internal secrecy
to some extent limited by so-called active choices. In terms of access to
information within a care provider's business, it follows from ch. § 4 HSLFFS 2016: 40 that the care provider “shall be
responsible for providing information on which others
care units or in which other care processes there is information about a certain
patient cannot be made available without the permission of the authorized user
a position on whether he or she has the right to take part in it
information (active selection). The information may then not be made available without
the authorized user makes another active choice. "
The fact that Capio requires active selection of its users does not mean that of employees
access to the personal data in the system has been limited in this way
way that they are no longer technically accessible to the user. It means
only that the user, in order for him to be able to access the information, must
"Click" in the journal system. This in turn means that all users
who make such active choices can take part in all patients' data and not
only the information that each user has a need to take part in.
The Data Inspectorate states that the Patient Data Act requires both
restriction of authorizations and active choices. The active selection function is one
privacy enhancing measure, but does not constitute such a restriction of

permissions referred to in ch. 4 Section 2 of the Patient Data Act. Of the preparatory work for
Patient Data Act, prop. 2007/08: 126, p. 149 states that the purpose of
the provisions are to imprint the obligation on the responsible care provider
to make active and individual eligibility assignments based on analyzes of

which details different staff categories and different types

businesses need. Because different users have different tasks

in different work areas, users need access to the data

limited to reflect this. The preparatory work shows that information

in addition, need to be stored in different layers so that more sensitive data is required

active choices or otherwise are not as easily accessible to staff as

less sensitive data.

Due to the above, the Data Inspectorate can state that they

active choices are not an access restriction according to ch. § 2

the Patient Data Act, as this provision requires that the competence must

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

tasks in health care.

Chapter 4 Section 4 of the Patient Data Act gives patients the right to request a block

the care documentation. However, a block is not such an access restriction

as referred to in ch. 4 Section 2 of the Patient Data Act, since a block is something like

requested by the patient himself. It is thus a position that does not

deals with the question of how the caregiver should restrict access to what

needed for the individual to be able to fulfill their duties within

Healthcare.

Capio St. Göran states that they use systematic log monitoring to

reduce the risk of employees improperly accessing patient information.

The Data Inspectorate states that the Patient Data Act does not provide anything

space for care providers to compensate for the absence of needs and risk analysis,

or an overly broad allocation of access rights, with an extensive

log follow-up.

With regard to the coherent record keeping in TakeCare, it appears that

Capio S: t Görans has limited the number of employees who have access to
the system to 606 employees. However, Capio St. Göran has not been made one
restriction on what documentation these employees can take
part of, so these employees have access to all personal data that
is processed in the journal system TakeCare, except for information such as

available at protected units at other care providers or the information that is
blocked by the patient according to ch. 6 the Patient Data Act.
That the allocation of authorizations in Cosmic, NPÖ and TakeCare does not have
preceded by a needs and risk analysis means that Capio S: t Görans does not have
analyzed users' needs for access to the data, the risks that
this access may entail and thus also not identified which
access that is justified to users based on such an analysis.
Users' reading permissions have thus not been restricted in such a way as
the provisions of the Patient Data Act require and Capio St. Göran has not, in
in accordance with Article 32 of the Data Protection Regulation, have used some
appropriate technical measures to restrict users' access to
patients' data in the medical record systems.
This in turn has meant that there has been a risk of unauthorized access and
unjustified dissemination of personal data partly within the framework of the internal
secrecy, partly within the framework of the coherent record keeping.
Capio S: t Görans has referred to the assessment that IVO has previously made in one
supervisory matter. Capio St. Göran emphasizes that IVO highlighted the importance of
employees with care assignments have sufficiently extensive qualifications for

NPÖ and TakeCare and the risks that could arise

patient safety if doctors and coordinating nurses would not

have sufficiently broad competence.

What emerges from IVO's review does not deprive Capio of its obligation to

carry out needs and risk analyzes as a basis for their allocation of competencies.

Because the analysis of needs and risks that Capio St. Göran has carried out

has not taken into account the risks to the rights of natural persons and

freedoms or the various kinds of risks that may be associated with one too

in case of availability regarding certain types of information, Capio S: t Görans does not have

demonstrated that reading privileges have been restricted in such a way as

the Data Protection Ordinance and the Patient Data Act require.

In summary, the Data Inspectorate can, in the light of what

appears from the investigation, state that Capio S: t Görans, neither within it

internal secrecy in Cosmic or the coherent record keeping in NPÖ and

TakeCare, has taken the appropriate technical or organizational measures

which they would have taken, in order to ensure a level of security that is

appropriate in relation to the risk posed by the treatment - in particular for

unauthorized access to personal data - in the journal systems Cosmic, NPÖ and

TakeCare.

In the light of the above, the Data Inspectorate can state that Capio S: t

Görans processes personal data in violation of Article 5 (1) (f) and Article 32 (1)

and 32.2 in the Data Protection Ordinance in that Capio St. Göran does not have

restricted users' permissions to access the journal systems

Cosmic, NPÖ and TakeCare, for what is only needed for the user

shall be able to fulfill their duties in health care in accordance with 4

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

This means that Capio S: t Görans has not taken measures to be able to

ensure and, in accordance with Article 5 (2) of the Data Protection Regulation, be able to:

show an appropriate security for the personal data.

Documentation of access (logs)

The Data Inspectorate can state that from the logs in Cosmic, NPÖ and

TakeCare provides information about the specific patient, which user

who has opened the record, measures taken, which

journal entry that has been opened, what time period the user has been

inside, all openings of the record made on that patient during it

selected time period and time and date of the last opening.

The Data Inspectorate finds that the documentation of the access (the logs)

in Cosmic, NPÖ and TakeCare are in accordance with the requirements set

appears from ch. 4 9 § HSLF-FS 2016: 40.

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.

The Data Inspectorate

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 in lieu of
other corrective measures referred to in Article 58 (2),
the circumstances of each individual case.

Article 83 (2) of the Data Protection Regulation sets out the factors to be taken into account
to decide whether to impose an administrative penalty fee, but also
what is to affect the size of the penalty fee. Of central importance to
the assessment of the gravity of the infringement is its nature, severity and
duration. In the case of a minor infringement may
the supervisory authority, in accordance with recital 148 of the Data Protection Regulation, issue a
reprimand instead of imposing a penalty fee.

Order

As mentioned, the health service has a great need for information in its
operations and in recent years has a very extensive digitization
occurred in healthcare. Both the data collections size and how many
sharing information with each other has increased significantly. This increases the demands on
the personal data controller, as the assessment of what is an appropriate
safety is affected by the extent of the 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 Capio S: t Görans has not taken action

appropriate security measures to protect the personal data in

the journal systems Cosmic, NPÖ and TakeCare by not complying with the requirements

which is set in the Patient Data Act and the National Board of Health and Welfare's regulations and thereby

does not meet the requirements of Article 5 (1) (f) and Article 32 (1) and (2) (i)

the Data Protection Regulation. The omission includes both the inner

the secrecy according to ch. 4 the Patient Data Act as the cohesive one

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

The Data Inspectorate therefore submits on the basis of Article 58 (2) (d)

the data protection ordinance Capio S: t Görans to implement and document

required needs and risk analyzes for the journal systems Cosmic, NPÖ and

TakeCare within the framework of both internal confidentiality and within the framework of

the coherent record keeping. Capio S: t Görans will continue, with the support of

these needs and risk analyzes, assign each user individually

authorization for access to personal data that is limited to what only

necessary for the individual to be able to fulfill his duties within

Healthcare.

Penalty fee

The Data Inspectorate can state that the violations basically concern Capio

St. Göran's obligation to take appropriate security measures to provide protection to 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 processing of data on patients in the main medical record system belong to the core of a healthcare provider activities, that the treatment includes many patients and the possibility of access refers to a large proportion of employees. Within the framework of the interior secrecy, more than 2,700 employees have access to relevant information close to 490,000 patients. In addition, it has more than 600 employees, within

the framework for the unified record keeping, the possibility of access to data concerning approximately 3 million patients in TakeCare.

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.
The maximum amount of the penalty fee in this case is EUR 20,000,000
or, in the case of a company, up to 4% of the total global
annual sales during the previous year, depending on the value
at most, in accordance with Article 83 (5) of the Data Protection Regulation.
The term "a 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 is considered to be 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

definitions of competition law. The rules for group liability in the EU

competition law revolves around the concept of economic unity. One

parent company and a subsidiary are considered part of the same financial

unit when the parent company exercises a decisive influence over the subsidiary.

The decisive influence (ie the control) can either be achieved through

ownership or by agreement. The case law shows that one hundred percent

ownership implies a presumption that control is to be considered to exist2.

Capio S: t Görans claims that according to the care agreement, which Capio Group

signed with the Stockholm Region, regarding the operation of St. Göran's Hospital shall

the company Capio St. Göran's Hospital is considered a completely independent business,

separate from Capio Group / Ramsay Générale de Santé, why turnover for

Capio Group and Ramsay Générale de Santé do not apply to Capio St.

Göran's Hospital.

The circumstances stated by Capio St. Göran in support of this are as follows.

Capio S: t Görans emphasizes that the current care agreement means that Capio S: t

Görans can not enter into agreements with other companies in the Capio Group as

gives rise to obligations for Capio St. Göran's without prior notice

in writing approved by the Stockholm Region. The Stockholm region has one

option right to repurchase all shares in Capio S: t Görans vid

the end of the care agreement. Capio St. Göran's activity content, patient volumes and compensation levels are determined exclusively by the Stockholm Region. Capio S: t Göran's owner company has no opportunities to influence these conditions by own decisions. Capio St. Göran's is separate from all other companies in The Capio Group in terms of IT infrastructure.

The Data Inspectorate assesses that the agreement clause that Capio S: t Görans invokes certainly indicates that Capio St. Göran should be kept separate and not mixed with the Group's other assets. The Data Inspectorate considers, however, that this does not show that Ramsay Générale de Santé and Capio S: t Göran does not constitute an economic entity in the manner referred to in the articles 101 and 102 of the TFEU. The data inspection is thus based on the above mentioned presumption and is based on the group Ramsay Générale de Santé: s annual turnover.

2

Case T-419/14 The Goldman Sachs Group, Inc. v European Commission

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.

Capio St. Göran's ability to pay is affected by the size of the business. The Data Inspectorate has calculated this based on the total global sales during the previous financial year for the Ramsay Group as Capio

St. Göran's is included in. According to the Group's annual report for the financial year

In 2018/2019, annual sales amounted to EUR 3,401 million.

The Data Inspectorate can state that the maximum penalty fee as

can be deleted is 136 million euros.

Based on the seriousness of the violations and that the administrative penalty fee

shall be effective, proportionate and dissuasive

The Data Inspectorate added the administrative sanction fee Capio S: t Görans to

30,000,000 (thirty million) kronor.

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 handled by Hans-Olof Lindblom, General Counsel, and the Head of Unit

Katarina Tullstedt participated.

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

Appendix: Appendix 1 - How to pay a penalty fee

Copy 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.