Decision

Diary no

2020-12-02

DI-2019-3846

The board of Capio St. Göran's Hospital

AB

St. Göransgatan 141

112 81 Stockholm

Supervision according to the data protection regulation and

the patient data act – needs and risk analysis and

questions about access in records systems

Table of Contents

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

The Swedish Data Protection Authority's decision

The Swedish Data Protection Authority has, during an inspection on April 3, 2019, found that Capio S:t Görans Sjukhus AB processes personal data in violation of article 5.1 f and 5.2, as well as article 32.1 0ch 32.2 of the data protection regulation1 by:

1.

Capio S:t Görans Sjukhus AB has not carried out needs and risk analyzes before assigning authorizations take place in the record systems Cambio Cosmic, National patient overview and TakeCare accordingly with 4 ch. § 2 and ch. 6 Section 7 of the Patient Data Act (2008:355) and Chapter 4. § 2 The National Board of Health and Welfare's regulations and general advice (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 taken appropriate organizational measures to be able to ensure and be able to demonstrate that the processing of the personal data has a security that is appropriate in relation to the risks.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection for natural persons with regard to the processing of personal data and on the free flow of such data and on the repeal of Directive 95/46/EC (general data protection regulation).

1

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

authorizations for access to the records systems Cambio Cosmic,

National patient overview and TakeCare to what only

is needed for the user to be able to fulfill their

tasks within health care in accordance with 4

Cape. § 2 and ch. 6 Section 7 of the Patient Data Act and ch. 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 the personal data.

Datainspektionen decides with the support of articles 58.2 and 83 i

the data protection regulation that Capio S:t Görans Sjukhus AB for

the violations of article 5.1 f and 5.2 as well as 32.1 and 32.2 i

data protection regulation must pay an administrative penalty fee of

30,000,000 (thirty million) kroner.

The Swedish Data Protection Authority orders with the support of Article 58.2 d

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

document the required needs and risk analyzes for the record systems

Cambio Cosmic, National patient overview and TakeCare and that thereafter,

with the support of these needs and risk analyses, assign each user

individual authorization for access to personal data which is limited to

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

tasks within the health and medical care, in accordance with article 5.1 f and

article 32.1 and 32.2 of the data protection regulation, ch. 4 § 2 and ch. 6 Section 7

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

Account of the supervisory matter

The Swedish Data Protection Authority initiated supervision by means of a letter on 22 March 2019 and

has inspected Capio S:t Görans Sjukhus AB on site on April 3, 2019 regarding their decisions on the allocation of authorizations have been preceded by a need-and risk analysis. The inspection has also included how Capio St. Görans has allocated authorizations for access to the main journal system Cambio Cosmic (below Cosmic) and the record systems National patient overview (hereinafter NPÖ) and TakeCare and what access possibilities the assigned permissions provide within both the framework of the internal secrecy according to ch. 4 patient data act, as the coherent record keeping according to ch. 6 the patient data act.

In addition to this, the Data Inspectorate has also reviewed the documentation of access (logs) contained in the records systems.

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

Due to what has emerged about Capio St. Göran's opinion i ask about restricting the read permission of its users in TakeCare, Capio S:t Görans was asked to comment specifically on what appeared in one statement from Karolinska University Hospital, which also uses TakeCare, where the technical possibilities regarding TakeCare were described.

What emerged in the case

Capio S:t Görans has essentially stated the following.

Personal data responsibility

Capio S:t Görans is a healthcare provider and personal data controller.

The business

Capio S:t Görans is a limited company that runs emergency hospitals according to a care agreement with Region Stockholm. Capio S:t Görans has 3,084 current 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 that Capio Group signed with Region Stockholm, regarding operation of St. Göran's Hospital, the company shall Capio St. Göran's Hospital is managed as a completely independent operation, separate from Capio Group/Ramsay Générale de Santé, hence turnover for Capio Group and Ramsay Générale de Santé is not applicable for Capio S:t Görans Hospital.

Journal system

Capio St. Görans has been using Cosmic as its main journal system since 2005 within the framework of internal confidentiality and for coherent record keeping within the Capio Group. In addition to this, Capio uses S:t Göran's NPÖ and TakeCare for consistent record keeping.

In the journal system Cosmic, there is personal data on 492,264 uniques patients. Cosmic has 2,764 active users. Capio St. Görans is included in the TakeCare record system together with a large number of other healthcare 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 record system.

Internal confidentiality

Needs and risk analysis

Capio S:t Görans has essentially 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. Against the background of this need and risk analysis, Capio St. Göran's guidelines for authorization allocation, which used by the operational managers when assigning authorizations.

In connection with the inspection on April 3, 2019, Capio stated S:t Görans that they had not decided when a needs and risk analysis should be carried out, but if a new event occurs – e.g. if a new clinic is opened - then it will be done a new needs and risk analysis. On March 19, 2020, Capio S:t Görans joined a document named “Needs and risk analysis, authorization profiles in Cosmic Clinical staff”, which is dated 14 January 2020.

Authorization assignment regarding access to personal data about patients

Capio S:t Görans has essentially stated the following.

Capio S:t Görans is divided into clinics and the operational managers are at respective clinic, which is responsible for assessing which authorization should assigned to the respective employee. Capio S:t Görans demands that the healthcare staff complies with the Patient Data Act when accessing patient data. Capio St. Görans has guidelines for authorization allocation which are drawn up according to a needs and risk analysis for authorization assignment according to set profiles in Cosmic.

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

means that the influx of patients and the tasks to be performed
mainly comes from the emergency department. In order for the emergency flow and
the emergency hospital assignment must be able to be carried out, broad allocations of
permissions. Capio S:t Görans emphasizes that they have a comprehensive
operations within emergency healthcare, with approximately 100,000 emergency visits per year. This
means that there is a very low percentage of pre-planned care at the hospital.
These guidelines state that they are hospital-wide and provide a framework for it
responsibilities, regarding assignment of access and authorization for record data. IN
the guidelines state that the term authorization refers to the technical
the possibility to share data, i.e. what an employee can do, not
what the employee may do in an individual case. The guidelines state that Capio
St. Görans has made the assessment that within the inner secrecy has as
rule all employees in close patient work at the hospital's clinics one
general need for access and thus authorization to these devices
collected documentation. Access to information outside respectively
area of activity requires active choices in the system. Patients with increased need
of privacy protection has the possibility of secrecy even between the traditional
the clinics by requesting a hold. However, this barrier can be broken.
However, according to the guidelines, a barrier may not be placed between clinics that
together participate in a common care process, or on such information
which must be available in all care processes at the hospital.
The guidelines state that the concept of permitted access refers to the question of when
it is permitted to take part in journal information, which mainly depends on
the employee's needs in the individual case and the guidelines specify a number
examples of situations where access is permitted. The guidelines thus contain
instructions that limit what employees may do within that space

for access to which they have been granted under the above paragraph, ie. the space that is technically possible to access within the "authority". According to these instructions, it is required that an employee participate in the care of a patient for that it must be permitted to share 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 granting authorization. Of these appear to be essentially similar judgments regarding the interior

the secrecy. The assessment is that the need to be able to assimilate clinical information about each patient is essential to be able to conduct healthcare with good quality and patient safety. Based on this, which rule all employees with clinical assignments access to Cosmics central functions. Access to information outside respectively area of activity requires active choices in the system. The risk that employees improperly have access to patient data reduced by configuration that requires active choices and regular and systematic log follow-up.

The business managers have the opportunity to receive support from chief physicians, 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 with the authorization structure. They do control of role and ordered profile before assigning permissions.

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 candidates. Capio St. Görans emphasizes that the employees who participate in work close to patients have a general need for all documentation at the hospital's clinics.

Employees can read all information in Cosmic. There are none limitations in access possibilities in the authorizations that Capio S:t Görans assigns the employees.

Active choices

Capio St. Görans 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 data relating to it clinic where the employee in question works, the so-called "home clinic". However, employees have the opportunity to access data 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 making one taking a position on whether he or she has the right to take part in this information. After an active selection, the user can click on to all information that exists about the patient within the framework of internal confidentiality at Capio S:t Görans, where the user can, among other things, take part in a "total journal" for the patient. Then the employee sees all information about the patient, except for the information that has been blocked.

Coherent record keeping

Capio S:t Görans has essentially 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. Against the background of this need and risk analysis, Capio St. Göran's guidelines for authorization allocation, which used by the operational managers when assigning authorizations.

On March 19, 2020, Capio S:t Görans received two documents named "Needs and risk analysis, eligibility profiles in NPÖ" and "Needs and risk analysis, reading permission in TakeCare". These documents are dated the 17 January 2020.

Authorization assignment regarding access to personal data about patients

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

Capio S:t Görans requires that the healthcare staff comply with the Patient Data Act at access to patient data, all access is logged and access is tracked through log controls.

Capio St. Göran's Hospital acts as personal data assistant for the others the caregivers within the Capio Group who use Cosmic and personal data assistant agreements are established regarding the provision of operation and management-related services. Employees at Capio S:t Görans can access patient data relating to the attention signal (UMS) for other companies within the Capio group. The attention signal shows information on warnings (medicines, foodstuffs), observanda, contagion and treatment/condition that needs attention (eg dialysis). Single patients' contact overview can be shown to users who with special choices specifies 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.

As far as the other journal systems are concerned, the normal course is to

the staff first uses Cosmic and then NPÖ. If

the information is missing in NPÖ, use of TakeCare may come into question. The

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

TakeCare.

A prerequisite for being able to access data in NPÖ or TakeCare is to

the employee is logged into Cosmic and is working with a specific patient. When

the employee then activates and logs into NPÖ or TakeCare,

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

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

the employee can access information relating to the patient in question.

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

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

possibility to take part in data in coherent record keeping, must be controlled

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

for local journals. Authorization should be offered to all doctors in clinical service

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

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

treat or plan for patients in the chain of care. In order to access

coherent record must be allowed, active consent from the patient is required.

The prerequisite for being asked for consent is that there is an ongoing,

planned or terminated care relationship and to obtain the data

contributes to the patient's health.

Capio S:t Görans states that they were subject to the Inspectorate for care and care's (IVO) supervision according to the Patient Safety Act, which referred to the review of how Capio S:t Görans ensures that patients receive the right medicine at enrollment to a care unit and discharge to another clinic. This one inspection was completed without criticism after Capio S:t Görans already described taken and planned measures that were intended, among other things, to ensure the access to medication information and medical record information of others care providers, mainly through TakeCare and NPÖ. Capio St. Görans emphasizes that IVO highlighted the importance of employees with care assignments having enough extensive authorization for NPÖ and TakeCare as well as what risks would could arise for patient safety if doctors and coordinating nurses would not have sufficiently broad authority.

NPÖ

In NPÖ, doctors and nurses in particular can take part in all of them information made available concerning the patient. If there are additional categories of people with employee assignments, these can also be given access. There is no possibility for the employee to search freely in NPÖ.

TakeCare

Eligibility for TakeCare is usually granted to doctors and other professional roles which has a special mission to coordinate care between Capio S:t Görans and other healthcare providers within the Stockholm Region.

In TakeCare, the "CapioRead" function is used. It is a finished authorization profile and there is no option to select another one

authorization profile, regardless of the employee's title. The right
means only a read authorization in TakeCare and it is mainly doctors who
is assigned to this as needed, but there may also be a need for others
people. All employees working in the emergency department as well as those
people who participate in the patient's later emergency flow have, for example
read permission in TakeCare. These people have access to all information in
TakeCare. However, this assumes that the employee clicks on journal filter i
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, to information belonging to Karolinska Hospital and SLSO
within Region Stockholm.

Capio S:t Görans emphasizes that they are Sweden's largest emergency department, by count
in patients per day. Since healthcare within the Stockholm Region does not use
the same main record system is used by NPÖ for coherent record keeping.
However, NPÖ lacks a number of types of information, above all
information about prescribed and administered medicines, why Capio S:t
In recent years, Görans also uses TakeCare, which is used by others
healthcare providers in the region. Analyzes of patient safety cases pointed out the shortcoming
on access to drug information as a negative factor. Access to
coherent record keeping is always preceded by consent, whenever possible
are collected and documented in the patient record.

Capio S:t Görans further states that the read rights in TakeCare have a filter
which primarily allows the reading of information that has arisen within Stockholms
county healthcare area or Karolinska hospital. The choice of care providers
is based on decisions about patient flows in the region's overall plan. In and
with Capio S:t Görans being an emergency hospital, you cannot know in advance which ones

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

the availability of information must be good to ensure a good and

patient-safe care. This means that 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 in order to take advantage of it

information needed to best care for a patient.

When accessing TakeCare, you must be logged into Cosmic on a specific

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

other social security number. All access is logged and access is tracked through

log controls.

Documentation of the access (logs)

Capio S:t Görans has mainly stated the following.

In Cosmic, the logs contain several categories of data, among others

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

patient chart, patient's name, gender, confidentiality, time of day (day, evening or night),

log clinic, log device, log user ID (name of the person, title and occupation),

module, which activity was performed, log argument (amount of information),

time stamp and date.

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

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. Görans supplemented the case with printed logs for Cosmic, NPÖ

and TakeCare.

When the Swedish Data Protection Authority received the printed logs for the respective

record system, the inspection was able to establish that when it came to the log extract

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

the measures have been taken. The Swedish Data Protection Authority requested that in supplementary

information from Capio S:t Görans be informed whether this information is

otherwise available.

In an opinion on March 19, 2020, Capio S:t Görans stated that there are two

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

both forms of log extracts are reported to the care unit. Capio St. Görans attached

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

it appears 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 May 25, 2018 and

is the primary legal regulation when processing personal data. This

also applies in healthcare.

The basic principles for processing personal data are stated in

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

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

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

including protection against unauthorized or unauthorized processing and against loss,

destruction or damage by accident, using appropriate

technical or organizational measures.

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

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

the principles in point 1 are complied with.

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

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

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

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

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

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

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

if necessary.

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

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

of the latest developments, implementation costs and treatment

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

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

take appropriate technical and organizational measures to ensure a

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

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

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

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

the personal data transferred, stored or otherwise processed.

Recital 75 states that when assessing the risk of natural persons

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

personal data subject to confidentiality, information about health or

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

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

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

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

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

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

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

the data processing involves a risk or a high risk.

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

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

Processing of personal data.

The Data Protection Regulation and the relationship with supplementary national

regulations

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

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

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

Provision of health care is one such task of generality

interest referred to in Article 6.1. e.

In healthcare, the legal bases can also; legal

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

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

interest and the exercise of authority are given to the Member States, according to Article

6.2, retain or introduce more specific provisions to adapt

the application of the provisions of the Regulation to national conditions.

National law can further determine specific requirements for data processing

and other measures to ensure legal and fair treatment. But

there is not only a possibility to introduce national rules but also a

duty; Article 6.3 states that the basis for the processing referred to in

paragraph 1 c and e shall be determined in accordance with Union law or

national law of the Member States. The legal basis may also include

special provisions to adapt the application of the provisions of

data protection regulation. Union law or Member States' national law

right must fulfill an objective of public interest and be proportionate to it

legitimate goals pursued.

Article 9 states that treatment of special categories of

personal data (so-called sensitive personal data) is prohibited. Sensitive

personal data includes, among other things, information about health. Article 9.2 states

the exceptions where sensitive personal data may still be processed.

Article 9.2 h states that processing of sensitive personal data may take place if

the processing is necessary for reasons related to, among other things

provision of healthcare on the basis of Union law or

Member States' national law or according to agreements with professionals on

health area and provided that the conditions and safeguards which

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

This means that both the legal bases public interest,

exercise of authority and legal obligation such as treatment of sensitive

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

supplementary rules.

Supplementary national regulations

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

the special conditions for processing personal data within health and

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

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

the law supplements the data protection regulation.

From ch. 1 Section 2 of the Patient Data Act states that the purpose of the Patient Data Act is to

information management within health care must be organized like this

that it caters for patient safety and good quality and promotes

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

processed 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 gain access to them.

The supplementary provisions in the Patient Data Act aim to

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

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

the information must be processed to meet patient safety as well as

privacy requirements.

The National Board of Health and Welfare has issued regulations with the support of the patient data regulation

and general advice on record keeping and processing of personal data i

health care (HSLF-FS 2016:40). The regulations constitute such

supplementary rules, which must be applied when healthcare providers treat

personal data in healthcare, see ch. 1 Section 1 of the Patient Data Act.

National regulations that supplement the data protection regulation's requirements for

security can be found in chapters 4 and 6. the Patient Data Act and chs. 3 and 4 HSLF-FS

2016:40.

Requirements to carry out needs and risk analysis

The care provider must according to ch. 4. § 2 HSLF-FS 2016:40 make a need-and

risk analysis, before assigning authorizations in the system takes place.

That an analysis of the needs as well as the risks is required is evident from the preparatory work

to the Patient Data Act, prop. 2007/08:126 pp. 148-149, as follows.

Authorization for the staff's electronic access to information about patients must be limited to

what the executive needs to be able to perform his duties in health and

healthcare. It includes, among other things, that authorizations must be followed up and changed or restricted accordingly

hand as changes in the individual executive's duties give rise to it.

The provision corresponds in principle to Section 8 of the Care Register Act. The purpose of the provision is to

inculcate the duty of the responsible health care provider to make active and individual

authorization assignments based on analyzes of which detailed information different

personnel categories and different types of operations need. But it is not only necessary

needs analyses. Risk analyzes must also be carried out where different types of risks are taken into account such as

may be associated with excessively wide availability regarding certain types of information.

Protected personal data marked confidential, information about publicly known persons,

data from certain clinics or medical specialties are examples of categories such as

may require special risk assessments.

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

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

categories of healthcare professionals to electronic access to records i

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

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

authority allocation should - even if it would have points from an efficiency point of view -

is considered an unwarranted dissemination of journal data within a business and should as such

not accepted.

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

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

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

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

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

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

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

limited to single persons.

Internal confidentiality

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

regulates employees' possibilities to electronically and automatically prepare

itself access to personal data that is electronically available in a

carer's organization (see prop. 2007/08:126 p. 141 and p. 239).

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

conditions for granting authorization to access such information about

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

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

tasks within health care.

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

users are assigned an individual authorization for access to

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

preceded by a needs and risk analysis.

Coherent record keeping

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

which means that a care provider - under the conditions stated in § 2 of the same

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

by other healthcare providers for purposes related to healthcare documentation. Access to

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

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

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

p. 247).

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

assignment and access control in the event of a joint operation

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

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

for consistent record keeping.

Documentation of access (logs)

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

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

automatically documented and systematically checked.

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

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

actions taken with data about a patient;

2. the logs show which care unit or care process

the measures have been taken,

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

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

The Swedish Data Protection Authority's assessment

Personal data controller's responsibility for security

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

general requirement for the personal data controller to take appropriate technical

and organizational measures. The requirement partly aims to ensure that

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

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

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

data protection regulation.

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

5.1 f and 32 of the data protection regulation.

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

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

relation to the risks to the rights and freedoms of natural persons which

the treatment entails. It is therefore necessary to identify the possible ones

the risks to the rights and freedoms of the data subjects and assesses

the likelihood of the risks occurring and the severity if they occur.

What is appropriate varies not only in relation to the risks but also

based on the nature, scope, context and purpose of the treatment. It has

thus meaning what kind of personal data is processed, how many
data, the question is, how many people process the data, etc.
Health care has a great need for information in its operations. The
it is therefore natural that the possibilities of digitization are utilized as much as possible
possible in healthcare. Since the Patient Data Act was introduced, one has a lot
extensive digitization has taken place in healthcare. As well as the data collections
size as how many people share information with each other has increased
substantially. This increase means at the same time that the demands on it increase
personal data controller, because the assessment what is an appropriate
safety is affected by the extent of processing.
There is also the issue of sensitive personal data. The data also concerns
people who are in a dependent situation when they are in need of care.
It is also often a question of a lot of personal data about each of these
people and the data may over time be processed by very
many people. All in all, this places great demands on it
personal data controller.
The data that is processed must be protected against external actors as well
the business as against unauthorized access from within the business. It appears
of article 32.2 that the personal data controller, when assessing the appropriate
security level, in particular must take into account the risks of accidental or illegal
destruction, loss or for unauthorized disclosure or access. In order to
able to know what is an unauthorized access it must
personal data controller is clear about what constitutes an authorized access.

Needs and risk analysis

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

A needs and risk analysis must partly contain an analysis of the needs, partly a analysis of the risks based on an integrity perspective that may be associated with an excessively wide allocation of authorization for access to personal data about patients. Both the needs and the risks must be assessed based on them

information that needs to be processed in the business, what processes it is the question of whether and what risks exist for the individual's integrity.

The assessments of the risks need to take place based on organizational level, there for example, a certain part of the business or task may be more more sensitive to privacy than another, but also based on the individual level, if that is the case the question of special circumstances that need to be taken into account, such as for example that it is a matter of protected personal data, generally known persons or otherwise particularly vulnerable persons. The size of the system also affects the risk assessment. It appears from the preparatory work for the Patient Data Act that the more comprehensive an information system is, the greater the variety permission levels there must be. (prop. 2007/08:126 p. 149).

It is thus a question of a strategic analysis at a strategic level, which should provide an authorization structure that is adapted to the business and this shall

be kept up to date.

In summary, the regulation requires that the risk analysis identifies

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

and how they affect the risk to the rights and freedoms of natural persons at Processing of personal data. This also applies to internal confidentiality as with coherent record keeping.

The risk analysis must also include special risk assessments, for example based on whether there are protected personal data that are classified as confidential, information about publicly known people, information from certain receptions or medical specialties (prop. 2007/08:126 p. 148149).

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

It is thus through the needs and risk analysis that it
data controller finds out who needs access, which
data the access possibility must include, at which times and in which
context the access is needed, and at the same time analyzes the risks to it
individual freedoms and rights that the processing may lead to. The result shall
then lead to the technical and organizational measures needed to
ensure that there is no access other than that which is necessary and
the risk analysis shows is justified.

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

At the time of the inspection on April 3, 2019, the Data Inspectorate requested a
documented needs and risk analysis. Capio St. Görans stated that they
previously carried out a needs and risk analysis, but that it did not
was preserved. Capio St. Göran stated that they in light of this
needs and risk analysis had produced guidelines for authorization allocation,
which must be used by the operational managers at each clinic when they
decides on the allocation of authorizations. Capio St. Görans has also developed
procedures for granting authorization. On March 19, Capio St. Görans gave

submitted new documents which are stated to be needs and risk analyzes concerning the three

the current medical record systems Cosmic, NPÖ and TakeCare.

The Swedish Data Protection Authority has described above which requirements apply during implementation

of a needs and risk analysis. In such a case, both the needs and the risks

assessed based on the information that needs to be processed in the business, which

processes it is a question of and which risks to the individual's integrity which

exists both on an organizational and an individual level. It is thus

the question of a strategic analysis at a strategic level, which should provide a

authority structure that is adapted to the operations.

The Swedish Data Protection Authority can state that neither the guidelines for the allocation of

authorization, the procedures for granting authorization or one of the three new ones

the documents listed as needs and risk analyzes contain any

assessment in terms of what needs different executives and different

kind of businesses need. A basic prerequisite for a

care providers must be able to meet the requirement to limit the electronic

the 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 carries out a needs and risk analysis.

There is also an analysis missing where Capio S:t Görans considers negatives

consequences for data subjects, different categories of data, categories of

registered and to what extent the extent of the number

personal and registered data affect the risk of 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 special missing

risk assessments based on whether it occurs, e.g. protected personal information

which are marked confidential, information about generally known persons, information

from certain practices or medical specialties or other factors

which require special protective measures. There is also no assessment of how

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

deemed to be.

The Swedish Data Protection Authority can state that the guidelines for the allocation of

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

the documents listed as needs and risk analyzes are missing one

basic inventory of user access needs and analysis of

risks, and there has also been no assessment of the users

actual needs in relation to the privacy risks that

the processing of personal data gives rise to

In summary, the Data Inspection Authority can state that either

the guidelines for the allocation of authority, the procedures for the allocation of

authorization or any 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 demonstrate that they have carried out a needs and risk analysis in the sense

referred to in ch. 4. § 2 HSLF-FS 2016:40, either

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

coherent record keeping, according to ch. 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 31.2 to be able

ensure and, in accordance with Article 5.2, be able to demonstrate that the processing of

the personal data has a security that is suitable in relation to the risks.

Authorization assignment regarding access to personal data about patients

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

a comprehensive processing of information about the health of individuals. This is done

especially valid in emergency healthcare. Notwithstanding this, access possibilities

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

the individual must be able to fulfill his duties.

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

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

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

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

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

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

unjustified dissemination of medical records within a business and should as

such is not accepted."

In healthcare, it is the person who needs the data in their work

who may be authorized to access them. This applies both within a

caregivers as between caregivers. It is, as already mentioned, through

the needs and risk analysis that the personal data controller finds out about whom

who needs access, which data the access should cover, at which

times and in which contexts the access is needed, and at the same time

analyzes which risks to the individual's freedoms and rights are

the treatment can lead to. The result should then lead to the technical and

organizational measures needed to ensure that no allocation

of authorization provides further access possibilities than the one that needs and
the risk analysis shows is justified. An important organizational action is to give
instructions to those who have the authority to assign permissions on how to do this
should go to and what should be taken into account so that, with the needs and risk analysis
as a basis, will be a correct authorization assignment in each individual case.
Capio S:t Görans emphasizes that their business is an emergency hospital. They do
regarding the need for broad assignments of authorizations in that it
is a very low percentage of pre-planned care in the hospital.

The Data Inspectorate does not dispute 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 permitted without prior need and
risk analysis assign all employees with clinical assignments such
covered access options. Capio S:t Görans is covered by an obligation
that, after carrying out needs and risk analyzes in the sense referred to in
4 ch. § 2 HSLF-FS 2016:40, assign each employee an individual
authorization that is limited to what he needs to be able to fulfill
their duties in health care.
In terms of internal secrecy, it appears that more than 2,700 employees
at Capio S:t Görans uses Cosmic, which contains information about approx
490,000 unique patients. It has emerged that Capio St. Görans does not have
limited user authorization for access to personal data within
the framework of the inner secrecy of the journal system Cosmic.

Capio S:t Görans has stated that the authorizations within the internal secrecy

to some extent limited by so-called active choices. As for access to

data within a healthcare provider's business, it follows from ch. 4 § 4 HSLFFS 2016:40 that the care provider "shall be

responsible for information on which other

care units or in which other care processes there is information about a certain

patient cannot be made available without the authorized user having done so

a position on whether he or she has the right to take part in this

information (active choice). The data must then not be made available without

the authorized user makes another active choice."

The fact that Capio requires active choices by its users does not mean that the employees'

access possibilities to the personal data in the system have been limited so

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 take part in the data, must

"click" your way through the journal system. This in turn means that all users

who make such active choices can access all patients' data and not

only the information that the respective user has a need to access.

The Swedish Data Protection Authority states that the Patient Data Act requires both

restriction of permissions and active choices. The active selection function is a

privacy-enhancing measure, but does not constitute such a limitation of

authorizations referred to in ch. 4 Section 2 of the Patient Data Act. Of the preparatory work to

patient data act, prop. 2007/08:126, p. 149 states that the purpose of

the provisions are to inculcate the obligation of the responsible care provider

to make active and individual authorization assignments based on analyzes of

which detailed information different staff categories and different types
businesses need. Because different users have different tasks
in different work areas, users need access to the data
be limited to reflect this. It appears from the preparatory work that data
also needs to be stored in different layers as more sensitive data requires
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. 4 Section 2
the Patient Data Act, as this provision requires the authorization to
is limited to what is needed for the individual to be able to fulfill their duties
tasks within health care.

4 ch. Section 4 of the Patient Data Act gives patients the right to request blocking
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, because a block is something that
requested by the patient himself. It is thus a stance that does not
addresses the issue of how the caregiver should limit access to what
is needed for the individual to be able to fulfill his duties within
Healthcare.

Capio S:t Görans states that they use systematic log follow-up to
reduce the risk of employees improperly accessing patient data.

The Swedish Data Protection Authority states that the Patient Data Act leaves nothing
space for healthcare providers to compensate for the absence of needs and risk analysis,
or an overly broad assignment of authority to access, with a comprehensive
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. Capio St. Görans, however, has not been made any
limitation in terms of what documentation these employees can take
part of, so these employees have access to all personal data that
processed in the TakeCare record system, except for information such as

is with protected units of other healthcare providers or the information that is
blocked by the patient according to ch. 6 the patient data act.
That the assignment 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 the users' needs for access to the data, the risks that
this access may entail and thus also not identified which
access that users are entitled to based on such analysis.
The users' read permissions have thus not been restricted in such a way as
the provisions of the Patient Data Act require and Capio S:t Görans does not have, i
in accordance with Article 32 of the Data Protection Regulation, used by some
appropriate technical measures to be able to limit users' access to
the patients' information in the 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
confidentiality, partly within the framework of coherent record keeping.
Capio S:t Görans has referred to the assessment that IVO previously made in one
supervisory matter. Capio S:t Görans emphasizes that IVO highlighted the importance of
employees with care assignments have sufficiently extensive authorization for

NPÖ and TakeCare and what risks could arise for

patient safety if doctors and coordinating nurses would not

have sufficiently broad authority.

What emerges in IVO's review does not relieve Capio of the obligation to

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

Because the analysis of needs and risks that Capio S:t Görans has carried out

have 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 a too

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

indicated that the read permissions have been restricted in such a way that

the data protection regulation and the patient data act require.

In summary, the Swedish Data Protection Authority can, against the background of what

appears from the investigation, state that Capio S:t Görans, whether within it

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

TakeCare, has taken the appropriate technical or organizational measures

that they would have taken, to be able to ensure a level of security that is

suitable in relation to the risk that the treatment entails - in particular for

unauthorized access to personal data – in the records systems Cosmic, NPÖ and

TakeCare.

Against the background 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 of the data protection regulation in that Capio S:t Görans does not have

limited user authorizations for access to the records systems

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

must be able to fulfill their duties in health and medical care according to 4

Cape. § 2 and ch. 6 Section 7 of the Patient Data Act and ch. 4 Section 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

demonstrate an appropriate level of security for the personal data.

Documentation of the access (logs)

The Swedish Data Protection Authority can state that the logs in Cosmic, NPÖ and

TakeCare shows information about the specific patient, which user

who has opened the record, actions 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

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

The Swedish Data Protection Authority states that the documentation of the access (the logs)

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

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

Choice of intervention

Legal regulation

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

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

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

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

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

specific period.

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

pursuant to Article 83 shall impose penalty charges in addition to or in lieu of

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

the circumstances of each individual case.

In article 83.2 of the data protection regulation, the factors that must be taken into account are stated for

to decide whether an administrative penalty fee should be imposed, but also

what will affect the size of the penalty fee. Of central importance to

the assessment of the seriousness of the violation is its nature, severity and

duration. If it is a question of a minor violation may

the supervisory authority, according to recital 148 of the data protection regulation, issue a

reprimand instead of imposing a penalty fee.

Order

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

business and in recent years has had a very extensive digitization

occurred in healthcare. Both the size of the data collections and how many there are

share information with each other has increased significantly. This increases the demands on

the personal data controller, because the assessment what is an appropriate

safety is affected by the extent of processing.

Within health care, this means a great deal of responsibility for it

personal data controller to protect the data from unauthorized access,

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

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

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

there is an actual analysis of the risks based on an integrity perspective

can occur in the event of an excessive assignment of authorization to access. From

this analysis must then be limited to the individual executive's access.

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

hand that changes in the individual executive's duties provide

reason for it.

The Data Inspectorate's supervision has shown that Capio S:t Görans has not taken action

appropriate security measures to provide protection to the personal data i

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

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

does not meet the requirements in Article 5.1 f and Article 32.1 and 32.2 i

data protection regulation. The omission includes the inner as well

confidentiality according to ch. 4 the Patient Data Act as the consolidated

record keeping according to ch. 6 the patient data act.

The Swedish Data Protection Authority therefore orders with the support of Article 58.2 d

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

required needs and risk analyzes for the records 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 analyses, assign each user individually

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

which is needed for the individual to be able to fulfill his duties within

Healthcare.

Penalty fee

The Swedish Data Protection Authority can state that the violations basically relate to Capio

St. Göran's obligation to take appropriate security measures to provide protection to personal data according to the data protection regulation.

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

Further aggravating circumstances are that the processing of information about patients in the master record system are at the core of a healthcare provider's business, that the treatment covers many patients and the possibility of access refers to a large percentage of employees. Within the framework of the inner the privacy department has more than 2,700 employees access to information relating to nearly 490,000 patients. In addition to that, more than 600 employees, within

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

When determining the seriousness of the violations, it can also be established that
the violations also include the fundamental principles of Article 5 i
the data protection regulation, which is among the more serious violations that can
give a higher penalty fee according to Article 83.5 of the Data Protection Regulation.
Taken together, these factors mean that the violations cannot be assessed
as minor infractions without infractions that should lead to one
administrative penalty fee.
The Swedish Data Protection Authority believes that these violations are closely related to
each other. That assessment is based on the fact that the needs and risk analysis must
form the basis for the assignment of the authorizations. The Swedish Data Protection Authority
therefore considers that these violations are so closely related to each other
that they constitute connected data processing according to Article 83.3 i
data protection regulation. The Swedish Data Protection Authority therefore determines a joint
penalty fee for these violations.
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 global total
the annual turnover in the previous year, depending on what the value is
maximum, according to Article 83.5 of the Data Protection Regulation.
The term "a company" includes all companies that conduct an economic
business, regardless of the entity's legal status or the manner in which it
be financed. A company can therefore consist of an individual company in the sentence one
legal person, but also by several natural persons or companies. Thus
there are situations where an entire group is treated as a company and its
total annual turnover shall be used to calculate the amount of a
breach of the Data Protection Regulation by one of its companies.
From consideration reason 150 in the data protection regulation appears, among other things

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

a company for this purpose is deemed to be a company within the meaning of

articles 101 and 102 of the TFEU[…]

This means that the assessment of what constitutes a company must be based on

competition law definitions. 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 economic

entity when the parent company exercises decisive influence over the subsidiary.

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

ownership or by agreement. Jurisprudence shows that one hundred percent

ownership means a presumption for control to be considered to exist2.

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

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

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

separated from Capio Group/Ramsay Générale de Santé, therefore turnover for

Capio Group and Ramsay Générale de Santé not applicable for Capio S:t

Göran's Hospital.

The circumstances Capio S:t Görans states in support of this are the following.

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

Görans cannot enter into an agreement with another company in the Capio group which

gives rise to obligations for Capio S:t Görans without that in advance

approved in writing by Region Stockholm. Region Stockholm has one

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

expiry of the care agreement. Capio St. Göran's business content, patient volumes
and compensation levels are determined exclusively by Region Stockholm. Capio St
Göran's ownership company has no opportunity to influence these conditions
through own decisions. Capio S:t Görans is separate from all other companies in
The Capio Group in terms of IT infrastructure.
The Data Inspectorate assesses that the contractual clause that Capio S:t Görans
invokes certainly indicates that Capio St. Görans should be held separately and not
mixed with the group's other assets. The Swedish Data Protection Authority
considers, however, that this does not show that Ramsay Générale de Santé and Capio S:t
Görans does not constitute an economic unit in the manner referred to in the articles
101 and 102 of the TFEU. The Swedish Data Protection Authority thus starts from the above
the said 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 must be effective, proportionate and
deterrent. This means that the amount must be determined so that it
the administrative sanction fee leads to correction, that it provides a preventive measure
effect and that it is also proportionate in relation to current as well
violations as to the solvency of the subject of supervision.
Capio S:t Göran's ability to pay is affected by the size of the business.
The Swedish Data Protection Authority has calculated this based on the total global
the turnover during the previous financial year for the Ramsay Group as Capio

St. Görans is included in. According to the group's annual report for the financial year

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

The Swedish Data Protection Authority can state that the maximum penalty fee which

can be issued is 136 million euros.

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

must be effective, proportionate and dissuasive determines

Datainspektionen the administrative penalty fee Capio S:t Görans to

30,000,000 (thirty million) kroner.

_____

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

presentation by IT security specialist Magnus Bergström. At the final

the handling is handled by chief legal officer Hans-Olof Lindblom 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 penalty fee

Copy to: The Data Protection Officer

How to appeal

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

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

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

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

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

examination.

You can e-mail the appeal to the Swedish Data Protection Authority if it does not contain any privacy-sensitive personal data or information that may be covered by secrecy. The authority's contact details appear on the first page of the decision.