The Swedish Data Protection Authority's guidance

Diary no: DI-2020-11495

Decision date: 2020-12-01

Needs and risk analysis in healthcare - a guide

Content

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Telephone: 08-657 61 00

Introduction

In the spring of 2019, the Swedish Data Protection Authority began supervision of eight healthcare providers within

health care for the purpose of, among other things, investigating the allocation of

authorizations in the caregivers' respective record systems have been preceded by needs and risk analyses. The reviews also

included how the allocation of

permissions implemented and what access capabilities they granted

the authorizations provide within the framework of, on the one hand, the internal secrecy according to ch. 4.

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

same team.

Needs and risk analyzes must form the basis for, among other things, authorization allocation and are of essential importance

for information about individuals and their

state of health must be protected and personal integrity maintained. The

central and generally applicable conclusions from the inspections regarding the requirements

on conducting needs and risk analyzes is summarized here

the guidance. The guidance aims to point out the importance of caregivers

ensures that appropriate needs and risk analyzes take place and to provide support to

healthcare providers in the implementation of such analyzes prior to awarding of

authorizations in journal system.

Applicable rules and the hierarchy of norms

The Data Protection Regulation the primary legal source

In order to protect the individual's privacy, there are common EU rules on

how personal data may be processed. The Data Protection Regulation, often abbreviated

GDPR1, was introduced on 25 May 2018 and is the primary legal regulation at

Processing of personal data. It contains 99 articles, which apply as

Swedish legislation and is supplemented by 173 considerations (reasons) as in parts

explains or clarifies the intent of the various articles. The provisions of

The data protection regulation applies to all processing of personal data within

Healthcare.

Before the data protection regulation was introduced, the Personal Data Act (PUL) applied.

Through PUL, an EU directive on the processing of personal data was introduced in 1998 i

Swedish law.2 PUL was secondary legislation and to that extent did not apply to others

1

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 95/56/EC (General Data Protection Regulation).

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of

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

such information.

2

rules regarding personal data processing were applicable. With the introduction of the data protection regulation, the hierarchy

of standards has changed centrally

manner when it comes to the processing of personal data. The Data Protection Ordinance is instead primary legislation and

sets basic rules for everything

personal data processing. The Regulation also regulates the role and responsibility of data protection authorities in monitoring

compliance with the Regulation. The

means that all Swedish legislation, when it comes to the treatment of

personal data, must have been adapted according to the regulation and that national rules

can only supplement and complete the data protection regulation.3

When personal data is processed, the provisions of the Data Protection Regulation on the protection of personal integrity must

therefore be applied in the first instance

taken into account and thereafter (with regard to the processing of personal data)

supplementary national legislation, such as the Patient Data Act,

be followed.

Basic principles must be followed and a legal basis must exist

The Data Protection Regulation states in Article 5 a number of basic principles for

processing of personal data, such as all covered by the regulation and

who handle personal data must comply. The principles concern requirements for legality,

transparency, purpose limitation, correctness, data minimization and

storage minimization.4

One of the basic principles concerns the requirement for security and means that

personal data must be processed in a way that ensures appropriate security

for the personal data using appropriate technical or organizational measures. Appropriate security must ensure, for example,

protection against

unauthorized or unauthorized processing, loss, destruction or damage by

accident.5

The personal data controller's responsibilities are also clarified in the data protection regulation. The so-called liability means

that it

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

the principles are complied with.6 The requirement partly aims to ensure that the processing of

the personal data is processed in accordance with the data protection regulation, partly that it

personal data controller must be able to demonstrate that the processing of

the personal data is processed in accordance with the regulation.

3

Complementary national legislation (or Union law regulation) presupposes its existence

provisions in the data protection regulation that allow deviating or supplementing

provisions of the data protection regulation.

4 Article 5.1.

5 Article 5.1 f.

6 Article 5.2.

3

4 (15)

The Data Protection Regulation and the relationship with supplementary national

regulations

As mentioned, one of the basic principles of the data protection regulation

legality.7 In order for the processing to be considered legal, it is required that there is a

legal basis.8 The legal bases that can be actualized in health and

healthcare is usually a matter of public interest, but also legal

obligation and exercise of authority may be relevant.9 Consent may as

rule not be used as a legal basis for processing personal data

in healthcare because there is an unequal relationship

between the care provider and the care recipient and a valid consent therefore cannot

be left.10

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

interest or exercise of authority may the Member States retain or

introduce more specific provisions to adapt the application of

the provisions of the data protection regulation to national conditions.

National law can further determine specific requirements for data processing

and other measures to ensure legal and fair treatment.11 Such

regulations exist for health care in the Patient Data Act and others

supplementary legislation relating to personal data processing in the field of healthcare.

Information about health constitutes sensitive personal data. Treatment of special

categories of personal data, so-called sensitive personal data, are as

main rule prohibited.

In the data protection regulation there are a number of exceptions that allow when sensitive

personal data may still be processed.12 Sensitive personal data may be processed

in healthcare if it is necessary to provide healthcare on the basis of either Union law or Member States'

7

Article 5.1 a.

Legal grounds are regulated in Article 6.

9 Article 6.1 c, e.

10 Consent can, however, many times, when the processing of personal data takes place on the basis of another

legal basis, be used as an integrity-enhancing measure.

11 Article 6.2. The Data Protection Ordinance also contains a requirement that the basis for

the processing referred to in paragraph 1 c and e shall be established in accordance with Union law or

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

provision to adapt the application of the provisions of the data protection regulation.

Union law or the national law of the Member States must fulfill an objective of general interest

and be proportionate to the legitimate aim pursued.

12 Article 9, 9.2 h.

8

national law or according to agreements with health professionals. One

prerequisite is that there is a regulated duty of confidentiality.13

Processing of personal data with the support of the legal bases in general interest, exercise of authority and legal obligation and processing of sensitive personal data requires that there is support for it in supplementary rules.

The Patient Data Act, the Patient Data Ordinance and the National Board of Health and Welfare's regulations contains supplementary national regulations

For Swedish purposes, both the basis for the treatment and the special ones the conditions for processing personal data in healthcare regulated in the Patient Data Act14 and the Patient Data Ordinance15. The Patient Data Act expressly states that the act supplements the data protection regulation. 16

It is clear from the Patient Data Act that the purpose of the act is that information management within health care must be organized so that it caters for patient safety and good quality and promotes cost-effectiveness.17 Furthermore, personal data is designed and otherwise processed so that that of patients and others data subject's privacy 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 made a balance regarding how the information should be processed to meet both the requirements for patient safety and the right to personal integrity in the processing of personal data.

The National Board of Health and Welfare has issued regulations with the support of the patient data regulation and general advice on record keeping and processing of personal data i health care (HSLF-FS 2016:40, regulations of the National Board of Health and Welfare).

The regulations constitute supplementary rules to be applied in the case of care providers processing of personal data in the health and medical care. 18

13

14

15

16

17

18

Article 9.3.

The Patient Data Act (2008:355).

The Patient Data Ordinance (2008:360).

1 ch. Section 4 of the Patient Data Act.

1 ch. Section 2 of the Patient Data Act.

1 ch. Section 1 subsection 2 of the Patient Data Act.

5

6 (15)

The personal data controller's responsibility for security when processing

personal data

That personal data controllers have a general responsibility to implement

appropriate technical and organizational measures to ensure and be able

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

the data protection regulation appears from the basic principles in article 5

but is also regulated in Article 24 of the regulation. The measures must be implemented with

consideration of the nature, scope, context and purpose of the processing as well as

the risks, of varying degrees of probability and seriousness, for the freedoms and rights of natural persons. The measures

must be reviewed and updated if necessary.

The controller's more precise responsibility for security in connection

with the processing of personal data is regulated in Article 32 of the regulation. The

personal data controller must take appropriate technical and organizational measures

measures to ensure a level of security appropriate in relation to

the risk. The assessment must take into account the latest developments,

the implementation costs, the nature, scope, context and

purposes as well as the risks to the rights and freedoms of natural persons, which may

be of varying degree of probability and severity. Special consideration must be given to them

risks that the processing entails, in particular for accidental or illegal

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

access to the personal data transferred, stored or otherwise

treated.

The Data Protection Regulation thus states that appropriate measures must be both

technical as well as organizational and that they must ensure a level of security that

is appropriate in relation to the risks to the rights and freedoms of natural persons that the processing entails. It is therefore

required that the person responsible for personal data firstly identifies the possible risks to the rights and freedoms of the data

subjects, and secondly assesses the likelihood of the risks occurring and

the severity if they occur. What is "appropriate" varies not only in

relationship to the risks, but also based on the nature, scope,

context and purpose. It is therefore important for the assessment which

technical and organizational measures that are appropriate for what it is

personal data that is processed, how much data is involved, how

many who process the data, for how long, etc.

Health care has a great need for information in its operations. Since

the Patient Data Act was introduced, a very extensive digitization has taken place within

care. Both the size of the data collections and how many people share

information with each other has increased significantly. That is also the question

sensitive personal data. The information concerns people who are in a

dependent situation when they are in need of care. It is also often a matter of many

personal data about each of these people and the data can over time

will be treated by many people in healthcare. This means that

the requirements for security increase because the assessment of what is appropriate

security, as described above, is affected by the nature and scope of the processing.

Here it is also central to emphasize that information processed within

care must be protected both against actors outside the business and against

unauthorized access from within the business then the risks, for example for accidental

or unlawful destruction, loss or unauthorized disclosure or unauthorized

access, also includes processing of actors within the business.

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

security is mainly found in chapters 4 and 6. the Patient Data Act and chs. 3 and 4

The National Board of Health and Welfare's regulations, HSLF-FS 2016:40.

A needs and risk analysis must be carried out before awarding of

authorization to record system takes place

The needs and risk analysis a central organizational security measure

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

conditions for granting authorization for access to data on patients

which is fully or partially automated. Such authorization shall be limited to

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

within health care.

Of ch. 4 § 2 The National Board of Health and Welfare's regulations follow that the care provider must be responsible for

that each user is assigned an individual authorization for access to

personal data. The healthcare provider's decision on the allocation of authorization must be preceded

of a needs and risk analysis. This means that national law prescribes requirements for an appropriate organizational security measure to be taken before awarding of authorizations to journal systems take place.

To carry out a needs and risk analysis that meets the requirements according to the data protection regulation and national legislation are primarily the question of a strategic analysis at a strategic level.

The needs analysis needs to be supplemented with an assessment of the risk of patients' freedoms and rights

This is evident, as reported, from the provisions of the Data Protection Ordinance on safety and is also highlighted in the preparatory work for the Patient Data Act and i The National Board of Health and Welfare's regulations that it is not only a question of needs analysis but also about risk analyzes in which different kinds of risks must be taken into account for

the freedoms and rights of individual natural persons that may result from an overly broad availability regarding certain types of data. 19

It is clear from the data protection regulation's considerations that the assessment of how likely and serious the risk to the data subject's rights and freedoms is should be determined based on the nature, scope, context and purpose. The risk should be evaluated on the basis of an objective assessment, through which it is determined whether the data processing involves a risk or a high risk.20

Factors that should be taken into account when assessing the risk to patients' rights and freedoms are, among other things, if it is the question of personal data that is covered of confidentiality, information about health or sexual life, if there is processing of personal data relating to vulnerable natural persons – above all children – or

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

number of registrants.21 Also protected personal data marked confidential, information about generally known persons,

information from certain receptions

or medical specialties are examples of categories of tasks that can

require special risk assessments.

Access must be limited to what each executive needs to

be able to perform their duties

According to ch. 4 Section 2 of the Patient Data Act must authorize the staff's electronic

access to information about patients is limited to what the executive

need to be able to carry out their tasks in health care.

According to the preparatory work, this includes, among other things, that authorizations must be followed up and

changes or is limited as changes in the individual

the executive's duties give reason for it.22 The purpose of

the provision was stated according to the preparatory work to be "inculcating the obligation for

the responsible caregiver to make active and individual

authorization assignments based on analyzes of which detailed information different

personnel categories and different types of operations need". Here it can be noted that

the preliminary works were written long before the data protection regulation, but that

the preliminary working statements correspond well with what now applies according to it

the basic principle of data minimization in the regulation.23

19

Prop. 2007/08:126 pp. 148–149.

Recital 76. Recitals 39 and 83 also contain writings that provide guidance on it more closely

the meaning of the data protection regulation's requirements for security when processing

personal data.

21 Reason 75 to the data protection regulation.

22 Prop. 2007/08:126 pp. 148–149. The provision in ch. 4 § 2 HSLF-FS 2016:40 corresponds to i

principle § 8 of the Care Register Act.

23 Article 5.1 c.

According to the preparatory work for the Patient Data Act, decisive for decisions on eligibility for, for example, different

categories of healthcare personnel to

electronic access to data in patient records be that the authorization must

limited to what the executive needs for the purpose of a good and safe

patient care. The preparatory work emphasizes that a more extensive or coarse meshed

authorization assignment should – even if it would have points from outside

efficiency point of view – is considered an unjustified dissemination of medical records

within a business and should not be accepted. Today, one fights too wide

authorization assignment against the basic principle of

task minimization

Different permission levels and layers to restrict access may be needed

When assigning authorization, it is clear from the preparatory work for the Patient Data Act

among other things, that there must be different authorization categories in the records system. 24

The more extensive an information system is, the more authorization levels

there must be.

According to operator statements, data should also be stored in different layers so that more

sensitive information requires active choices or is otherwise not as easily accessible

for the staff as less sensitive data. It may be noted here that use of active choices does not in itself constitute such limitation of

eligibility as

referred to in ch. 4 Section 2 of the Patient Data Act. This provision requires that the authorization be limited to what is needed

for the individual to be able to fulfill

their duties in health care, i.e. only those who

have a need for data must have access to them. For an employee

who must have access to certain, particularly sensitive, data must, however

active elections be used as an integrity-enhancing measure, by ensuring

that conscious decisions are required before access takes place

the data.

In the case of personnel who work with business monitoring, statistical production, central financial administration and similar

activities such as

is not individual-oriented, probably according to the majority of executives

the preparatory work is sufficient with access to information that can only be derived indirectly

to individual patients. Electronic access to code keys, social security number

and other information that directly identifies individual patients should on this

area, according to the preliminary work, could be strongly limited to single people.

When a need and risk analysis is missing prior to the assignment of authorization in one

record system in health care, there is no basis for it

24

Prop. 2007/08:126 pp. 148-149.

9

1 0 (15)

personal data controllers in a legal way must be able to assign their users

a correct authorization. The personal data controller is responsible for, and shall

have control over, the processing of personal data that takes place within the framework of

the business. To assign users a when accessing records system, without

that this is based on a performed needs and risk analysis, means that it

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

system, nor can he demonstrate that he has

the required control.

The requirement for a needs and risk analysis includes both the so-called internal

the area of confidentiality and coherent record keeping

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

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

operations and especially employees' opportunities to prepare access to

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

organisation. As mentioned, a care provider has according to ch. 4 Section 2 of the Patient Data Act

to determine conditions for granting authorization for access to such

information about patients that is fully or partially automated. Such

authorization must be limited to what is necessary for the individual to be able to

fulfill their duties in health care. The requirement for one

needs and risk analysis naturally includes employees who are in

the care provider's organization.25

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

This means that a care provider - under the conditions specified in ch. 6 Section 2

patient data act - may have direct access to personal data processed by

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

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

the healthcare provider registers whether the patient is available to other healthcare providers who

participates in the coherent record keeping.26 Of ch. 6. Section 7 of the Patient Data Act

it follows that the regulations in ch. 4 Section 2 also applies to authorization allocation

in case of coherent record keeping. The requirement for the care provider to carry out a

needs and risk analysis before assigning authorizations in the system takes place, applies

thus also in systems for coherent record keeping.

25

26

See also prop. 2007/08:126 p. 141ff and p. 239.

Prop. 2007/08:126 p. 247.

10

1 1 (15)

Implementation of the needs and risk analysis – six steps

The section gives an overview of the six steps that should be followed when need and the risk analysis is carried out.

The six basic steps of the needs and risk analysis.

1. Analyze and determine the needs of the business

2. Identify and analyze the risks to individuals' personal integrity

3. Identify and take appropriate technical and organizational measures to reduce the risks

4. Determine, based on the analyses, an authorization structure that supports the needs and minimizes the risks

5. Document all steps

6. Continually review the authorization structure and what the actions are appropriate to reduce the risks.

A needs and risk analysis usually begins with an analysis of the needs.

The business's need for access to information about patients in order to be able to offer adequate care is determined through the analysis, and must include what employees need to be able to fulfill their duties. Need and the risk analysis must also, as described in the previous section, include a analysis of risks based on an integrity perspective that may be associated with an excessive when granting authorization to access patient data.

The risk analysis must include an objective assessment of how likely and serious
the risk to the rights and freedoms of the data subjects is and in any case determine
whether it is a question of a risk or a high risk.
It is through the needs and risk analysis that the person in charge of personal data takes
find out who needs access, what data the access option should
include, at which times and in which contexts or processes
the access is needed. At the same time, the risks to the individual's freedom and
rights that the processing may lead to.
The analysis should then lead to identifying the technical and organizational ones
measures needed to be able to grant the necessary authorizations, and
ensure that no assignment of authority provides further access opportunities
than the need and risk analysis shows is justified. These technical and
organizational measures must then be implemented.
The strategic analysis must result in an authority structure that is
adapted to the needs of the business both organizationally and individually
level. This needs to result in instructions on authorization allocation which
then implemented. An important organizational measure is thus to give instructions

to those who have the authority to assign permissions on how this should be done and
what must be taken into account so that, with the needs and risk analysis as a basis, it becomes
a correct authorization assignment in each individual case.
A well-developed documentation of performed analyzes and assessments is
central for the care provider to be able to demonstrate that the authorization assignment is
expedient and fulfills the requirements set according to
the data protection regulation, the patient data act and the regulations of the National Board of Health and Welfare.

To the extent that a business is not static, authorizations are a perishable commodity. In order to

ensure correct authorization assignment needs assigned authorizations

is continuously checked and the authorization structure is continuously kept up to date. 27

As has already been emphasized, a needs and risk analysis forms the basis for

the personal data controller in a legal way must be able to assign his

user a correct authorization. It is also the basis for the personal data controller's control over the personal data processing that

takes place in

the records system and that he can show that he has the required control.

Consequences of not carrying out a needs and risk analysis

As mentioned, the needs and risk analysis is fundamental to a correct

authorization assignment must be possible.

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

risk analysis means that the data controller has not analysed

the users' need for access to the data, the risks that this access poses

can entail and thus also not identified which access possibilities are

are entitled to assign the users. In such cases, the person responsible has not used

take appropriate measures to restrict permissions for access to

the journal system to only what is needed for the user to be able to

fulfill their duties in health care.

If the lack of analysis leads to too narrow an allocation of permissions, it can

lead to staff not being able to take part in the tasks they need to perform

their work, which poses a risk to the patient's life and health.

If the lack of analysis instead leads to the users' permissions not

are limited to what is only necessary for them to be able to fulfill their duties

tasks, it can lead to the tasks ending up in the wrong hands and

used for unauthorized purposes. That the patient's right to privacy is not respected

27

4 ch. Section 3 HSLF-FS 2016:40.

12

1 3 (15)

can affect patients' trust in care. That, in turn, can have an effect

both patients' willingness to share data, as well as patients' willingness to leave

correct and complete information to their healthcare provider. In a report from

the authority for health care analysis states 8 percent of

the respondents in a survey that they have withheld information out of concern for over

that someone else could see the data. Another 8 percent state that

they considered it.28

It is therefore essential for healthcare to have one

authority structure that has its basis in well-executed needs and

risk analyzes so that users are neither assigned too broadly nor too narrowly

authorizations for access to the records systems.

Because a needs and risk analysis is a prescribed organizational action

which must be taken before the assignment of authorizations takes place, it can also lead to

legal consequences if the controller fails to implement

needs and risk analyses.

In such a case, the person in charge of personal data has not used suitable ones

measures to limit user access to patients' data i

the journal system to what is only needed for the user to be able to

fulfill their duties in health care. This contradicts both

against the principle of data minimization according to Article 5.1 c

the data protection regulation and the requirement to ensure appropriate security for

the personal data, including protection against unauthorized access or unauthorized

treatment according to article 5.1 f, which is also apparent from article 32, which against ch. 4

Section 2 of the Patient Data Act and ch. 4 § 2 Regulations of the National Board of Health and Welfare.

Can the personal data controller not show that the provision on data minimization is followed and that the personal data

controller has taken measures to

be able to ensure appropriate security for the personal data, it has

personal data controller also not fulfilled the responsibility according to article

5.2 of the data protection regulation.

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

Datainspektionen a number of corrective powers to be available. 29

The supervisory authority can, among other things, subpoena the person in charge of personal data

to ensure that the processing takes place in accordance with the regulation and if required

in a specific way and within a specific period.

The authority for care and care analysis report For safety's sake - The population's

attitude towards benefits and risks of digital health data 2017:10 pp. 76-77

29 Article 58.2 a–j of the data protection regulation.

It follows from Article 58.2 of the data protection regulation that the supervisory authorities, i

Sweden Datainspektionen30, in accordance with Article 83 shall impose

penalty fees in addition to, or in lieu of, other corrective actions

depending on the circumstances of each individual case. Penalty fees according to

the data protection regulation are not insignificant and must be effective,

proportionate and dissuasive. A possible penalty fee may within

the care area for the same violation entail completely different outcomes, depending

whether it is a question of a private or public healthcare provider.

Depending on whether the violation relates to articles covered by Article 83(4) or
83.5 of the data protection regulation, the penalty fees can be of varying amounts. At
Violation of more central articles may penalize companies
amount to EUR 20 million or to a maximum of 4 percent of the global
the annual turnover during the previous budget year, depending on the amount
is highest. Alternatively, the maximum limit for the sanction amount is EUR 10 million
or a maximum of 2 percent of the global annual turnover in the previous year
budget year, depending on which amount is the highest.
For authorities, national rules may state that authorities can be imposed
administrative penalty fees.31 According to ch. 6 Section 2 of the Data Protection Act can
sanction fees are decided for authorities, but up to a maximum of SEK 5 million
alternatively SEK 10 million depending on whether the violation concerns articles
which is covered by article 83.4 or 83.5 of the data protection regulation.
When it comes to violations of fundamental principles and sensitive
personal data is updated to the higher scale of the penalty fees. 32
Article 83.2 of the data protection regulation shows the factors that the Data Protection Authority has to take into account when deciding whether an administrative penalty fee
must be imposed, but also what will affect the size of the penalty fee. Of
of central importance for the assessment of the seriousness of an infringement is its character,
severity and duration as well as the degree of responsibility of the personal data controller (and personal data assistant) taking into account the technical and
organizational measures carried out in accordance with the data protection regulation.33

30
As of January 1, 2021, Datainspektionen will change its name to
The Swedish Privacy Protection Authority.
31 Article 83.7 of the data protection regulation.

32 Article 83.5 a of the data protection regulation.

33 Among other things, Article 32 of the data protection regulation.

If it is a minor violation, the supervisory authority may issue one

reprimand instead of imposing a penalty fee.34 Failure to implement a

needs and risk analysis prior to the allocation of authorizations is no less important

violation.

In summary, it can be stated that it is of central importance that

personal data controller performs a needs and risk analysis before assigning

permissions take place. It is a matter of sensitive personal data, often large

data collections, many have access to the data and the risk to them

basic freedoms and rights of the registered person if data is disclosed without authorization

is usually relatively high. Lack of a needs and risk analysis which

has led to an overly broad or coarse-grained allocation of authority entails

usually that a penalty fee must be paid.

34

Reason 148 to the data protection regulation.