The Data Inspectorate's guidance

Diarienr: DI-2020-11495

Decision date: 2020-12-01

Needs and risk analysis in health care - a guide

Content

Postal address: Box 8114, 104 20 Stockholm

Website: www.datainspektionen.se

E-mail: datainspektionen@datainspektionen.se

Phone: 08-657 61 00

Introduction

In the spring of 2019, the Data Inspectorate began inspecting eight care providers within

health care in order, among other things, to investigate whether the allocation of

authorizations in the caregivers' respective medical record systems have been preceded by needs and risk analyzes. The

reviews also included how the allocation of

privileges have been completed and the access options they have been granted

within the framework of the internal secrecy according to ch.

the Patient Data Act, and the cohesive record keeping according to ch.

same team.

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

information on individuals and their

health conditions 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 are summarized in this

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

ensures that appropriate needs and risk analyzes are carried out and that support is provided

caregivers in carrying out such analyzes prior to the award of

permissions in journal systems.

Applicable rules and the hierarchy of norms

The Data Protection Regulation is the primary source of law

To protect the individual's privacy, there are EU common rules on

how personal data may be processed. 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 are valid as

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

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

The Data Protection Regulation applies to all processing of personal data within

Healthcare.

Before the Data Protection Ordinance was introduced, the Personal Data Act (PUL) applied.

The PUL introduced in 1998 an EU directive on the processing of personal data in

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 protection

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

of such information and repealing Directive 95/56 / EC (General Data Protection Regulation).

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 concerning the processing of personal data were applicable. With the introduction of the Data Protection Regulation, the

hierarchy of standards has changed at a central level

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

out basic rules for all

personal data processing. The regulation also regulates the role and responsibilities 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 to the Regulation and that national rules

can only supplement and complete the Data Protection Regulation.3

Therefore, when processing personal data, the provisions of the Data Protection Regulation on the protection of personal

privacy must come first

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

supplementary national legislation, such as the Patient Data Act,

followed.

Basic principles must be followed and there must be a legal basis

Article 5 of the Data Protection Regulation sets out a number of basic principles for:

processing of personal data, as all covered by the Regulation and

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

transparency, purpose limitation, accuracy, data minimization and

storage minimization.4

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

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

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

protection against

unauthorized or unauthorized treatment, loss, destruction or damage by

accident.5

The responsibility of the data controller is also clarified in the Data Protection Ordinance. The so-called liability means that it

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

the principles are complied with.6 The requirement is partly to ensure that the treatment of

the personal data is performed in accordance with the Data Protection Regulation, partly that it

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

personal data are performed in accordance with the Regulation.

Supplementary national legislation (or Union law) presupposes that it exists

provisions of the Data Protection Regulation that allow derogations or supplements

provisions of the Data Protection Regulation.

Article 5.1.

Article 5.1 f.

Article 5.2.

3

4 (15)

The Data Protection Regulation and the relationship with complementary national

provisions

As mentioned, one of the basic principles of the Data Protection Regulation

legality.7 In order for the treatment to be considered legal, it is necessary that there is one

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

Healthcare is usually a task of general interest, but also legal

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

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

in health care because there is an unequal relationship

between the care provider and the care recipient and a valid consent therefore can not

left.10

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

interest or exercise of authority, Member States may retain or

introduce more specific provisions to adapt the application of

the provisions of the Data Protection Regulation to national circumstances.

National law may lay down specific requirements for the processing of data

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

There are provisions for health and medical care in the Patient Data Act and others

supplementary legislation relating to the processing of personal data in the field of health and medical care.

Health information constitutes sensitive personal data. Treatment of special

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

general rule prohibited.

The Data Protection Regulation contains a number of exceptions that allow when sensitive

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

in health care if it is necessary to provide health care on the basis of either Union law or that of the Member States;

7

Article 5.1 a.

Legal bases are governed by Article 6.

9 Article 6.1 c, e.

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

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

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

the treatment referred to in paragraph 1 (c) and (e) shall be determined in accordance with Union law or

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

provision to adapt the application of the provisions of the Data Protection Regulation.

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

and be proportionate to the legitimate aim pursued.

12 Article 9, 9.2 h.

8

national law or in accordance with agreements with health professionals. One

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

Processing of personal data on the basis of the legal bases in general

interest, exercise of authority and legal obligation as well as treatment 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 provisions

In the case of Sweden, both the basis for the treatment and the special ones

the conditions for processing personal data in the health care system

regulated in the Patient Data Act14 and the Patient Data Ordinance15. The Patient Data Act explicitly states that the law complements the Data Protection Ordinance.16

The Patient Data Act states that the purpose of the law is to handle information

in health care must be organized so that it meets patient safety and good quality and promotes cost-effectiveness.17

Furthermore,

personal data is designed and otherwise processed so that patients and others

the privacy of the data subject is respected. In addition, documented personal data must be handled and stored so that unauthorized persons do not have access to them.

The supplementary provisions in the Patient Data Act aim to take care of both privacy protection and patient safety. The legislature has thus

through the regulation made a balance in terms of how the information should be

treated to meet both the requirements for patient safety and the right to

privacy in the processing of personal data.

The National Board of Health and Welfare has, with the support of the Patient Data Ordinance, issued regulations

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

health care (HSLF-FS 2016: 40, National Board of Health and Welfare regulations).

The regulations constitute supplementary rules that must be applied to care providers

processing of personal data in health care.18

14

15

16

17

18

Article 9.3.

Patient Data Act (2008: 355).

Patient Data Ordinance (2008: 360).

1 chap. Section 4 of the Patient Data Act.

1 chap. Section 2 of the Patient Data Act.

1 chap. 1 § 2 paragraph of the Patient Data Act.

5

6 (15)

Personal data controller's responsibility for the security of processing

personal data

That data controllers have a general responsibility to implement

appropriate technical and organizational measures to ensure and be able to

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

The Data Protection Regulation is set out in the basic principles set out in Article 5

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

taking into account the nature, scope, context and purpose of the treatment and

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

be reviewed and updated as necessary.

The more precise responsibility of the data controller for security in connection

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

personal data controllers shall take appropriate technical and organizational measures

measures to ensure a level of safety appropriate to:

the risk. The latest developments shall be taken into account in the assessment,

implementation costs, nature of the treatment, scope, context and

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

be of varying degree of probability and seriousness. Special consideration must be given to those

risks posed by the treatment, in particular to unintentional 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 and 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 treatment entails. It is therefore

necessary that the person responsible for personal data identifies the possible risks to the data subjects' rights and freedoms,

and assesses the probability that the risks will occur and

severity if they occur. What is "appropriate" does not only vary in

in relation to the risks but also based on the nature, scope,

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

technical and organizational measures appropriate to what it is for

personal data processed, how much data is in question, how

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

The health service 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 share

information with each other has increased significantly. It is also a question of

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

dependency situation when they are in need of care. It is also often a question of many

personal data of each of these persons and the data may over time

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

the requirements for safety increase as the assessment of what is appropriate

safety, as described above, is affected by the nature and extent of the treatment.

Here it is also central to emphasize that data that is processed within

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

unjustified access from within the business when the risks, for example too unintentional

or unlawful destruction, loss or unauthorized disclosure or unauthorized use

access, also includes the treatment of actors within the business.

National provisions that supplement the requirements of the Data Protection Regulation

security is found mainly in Chapters 4 and 6. the Patient Data Act and Chapters 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 allocation of

access to journal systems takes place

The needs and risk analysis is a central organizational security measure

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

conditions for granting access to patient data

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

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

in health care.

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

that each user is assigned an individual privilege to access

personal data. The care provider's decision on the allocation of eligibility 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 allocating

permissions 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 in the first instance the question of

a strategic analysis at the strategic level.

The needs analysis needs to be supplemented with an assessment of the risk of

patients' freedoms and rights

It appears, as reported, from the provisions of the Data Protection Ordinance on

safety and is also emphasized in the preparatory work for the Patient Data Act and in

The National Board of Health and Welfare's regulations that it is not just a question of needs analyzes but

although risk analyzes in which different types of risks must be taken into account

the freedoms and rights of individuals that may result from an excessive

availability of certain types of data.19

It is clear from the Data Protection Regulation's considerations that the assessment of

the probable and serious risk to the data subject's rights and freedoms

should be determined on the basis of the nature, extent, context and

purpose. The risk should be evaluated on the basis of an objective assessment,

by 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 a question of personal data that is covered

of duty of confidentiality, information on health or sexual life, if there is treatment of

personal data concerning vulnerable natural persons - in particular children - or

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

number of registered.21 Also protected personal data that is classified, information about publicly known persons, data from certain receptions or medical specialties are examples of categories of data that can require special risk assessments.

Access shall be restricted to what each executive needs to be able to perform their duties

According to ch. 4 Section 2 of the Patient Data Act shall have competence for the staff's electronic access to patient information is limited to what the executive need to be able to perform their duties in health care.

According to the preparatory work, this means, among other things, that authorizations must be followed up and change or diminish over time as changes in the individual the executive's duties give rise to it.22 The purpose of the provision was stated according to the preparatory work to be to “imprint the obligation for the responsible caregiver to make active and individual eligibility assignments based on analyzes of which details are different staff categories and different types of activities need ”. Here it can be noted that the preparatory work was written long before the Data Protection Ordinance, but that the preparatory statements are in good agreement with what now applies under it basic principle of data minimization in the Regulation.23

19

Prop. 2007/08: 126 pp. 148–149.

Recitals 76. Recitals 39 and 83 also contain writings that provide guidance on this in more detail the meaning of the Data Protection Regulation's requirements for security in the processing of personal data.

21 Recital 75 of the Data Protection Regulation.

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

principle Section 8 of the Health Care Register Act.

23 Article 5.1 c.

20

8

9 (15)

According to the preparatory work for the Patient Data Act, decisive decisions for eligibility for, for example, different categories of health care staff should be

electronic access to information in patient records be that the authorization should

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

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

eligibility should - even if it would have points from outside

efficiency point of view - is considered an unjustified dissemination of journal information

within a business and should not be accepted. Today one is fighting too hard

allocation of competences against the basic principle of

task minimization

Different permission levels and layers to restrict access may be needed

When allocating authority, it appears from the preparatory work for the Patient Data Act

among other things, that there should be different authorization categories in the medical record system.24

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

there must be.

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

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

for staff as less sensitive tasks. It can be noted here that the use of active choices does not in itself constitute such a restriction of competence as

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

necessary for the individual to be able to fulfill

their duties in health care, that is, only those who

need information must have access to it. For an employee

which shall have access to certain, particularly sensitive, data shall, however

active choices are used as a privacy enhancing measure, by ensuring

that conscious positions are required before access is made to

the data.

In the case of staff working with business follow-up, statistical production, central financial administration and similar activities

such as

is not individual-oriented, it should for the majority of executives according to

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 data that directly point out individual patients should on this

area, according to the preparatory work, could be severely limited to individuals.

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

medical records system, there is no basis for it

24

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

9

1 0 (15)

personal data controllers must be able to legally assign to their users

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

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

the business. To assign users a wide access to journal system, without

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

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

nor can he show that he has

the control required.

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 the internal secrecy, that is

say regulates how the privacy protection is to be handled within a care provider

activities and especially employees' opportunities to prepare for access to

personal data that is electronically available in a healthcare provider

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

to determine the conditions for granting access rights to such

data on patients who are fully or partially automated. Such

eligibility shall be limited to what is necessary for the individual to be able to

fulfill their duties in health care. The requirement of one

needs and risk analysis naturally includes employees who are in

the caregiver's organization.25

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

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

Patient Data Act - may have direct access to personal data processed by

other care providers for purposes related to care documentation. The access to

information is provided by a care provider making information about a patient who

the caregiver registers if the patient is available to other caregivers who

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

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

in the case of unified record keeping. The requirement that the caregiver must perform one

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

thus also in systems for coherent record keeping.

26

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

Prop. 2007/08: 126 pp. 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 needed and the risk analysis is carried out.

The six basic steps of needs and risk analysis.

1. Analyze and determine the needs of the business

2. Identify and analyze the risks to individuals' privacy

3. Identify and take appropriate technical and organizational measures to:

reduce the risks

4. Based on the analyzes, establish a competency structure that supports the needs and minimizes risks

5. Document all steps

6. Continuously review the authorization structure and what measures are in place suitable for reducing risks.

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

The business's need for access to patient information in order to be able to offer adequate care is determined by the analysis, and should include what employees need to be able to fulfill their duties. Needs and the risk analysis shall also, as described in the previous section, include a analysis of risks from an integrity perspective that may be associated with one too when allocating access to patient data.

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

the risk to the data subjects' rights and freedoms is and in any case determined

whether it is a matter of a risk or a high risk.

It is through the needs and risk analysis that the person responsible for personal data takes

find out who needs access, what information the access option should be

include, at what times and in what contexts or processes

access is needed. At the same time, the risks to the individual's freedom and

rights that the treatment may lead to.

The analysis should then lead to the identification of the technical and organizational

measures necessary to be able to provide the necessary authorizations, and

ensure that no allocation of privileges provides further access possibilities

than that shown by the needs and risk analysis is justified. These technical and

organizational measures must then be implemented.

The strategic analysis should result in a competency structure that is

adapted to the needs of the business, both organizationally and individually

level. This needs to result in authorization assignments as

then carried out. An important organizational measure is thus to provide instructions

to those who have the authority to confer powers on how to proceed and

what is to be taken into account so that it, with the needs and risk analysis as a basis, becomes

a correct authorization allocation in each individual case.

A well-worked documentation of analyzes and assessments made is

central for the care provider to be able to show that the allocation of eligibility is

appropriate and meets the requirements set out in

the Data Protection Ordinance, the Patient Data Act and the National Board of Health and Welfare's regulations.

To the extent that an activity is not static, authorizations are a fresh product. In order to

ensure a proper authorization assignment needs assigned privileges

continuously checked and the authorization structure is continuously updated.27

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

the person responsible for personal data must be legally able to assign his

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

place in

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

Consequences of not having a needs and risk analysis carried out

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

it must be possible to grant authorization.

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

risk analysis means that the person responsible for personal data has not analyzed

users' need for access to the data, the risks associated with that access

can entail and thus also not identified which access options

are justified to assign users. The person responsible has not used in such cases

take appropriate measures to restrict 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 a too narrow allocation of competencies, it can

lead to staff not being able to access 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

limited to what is only needed for them to be able to fulfill theirs

tasks, it can lead to the tasks falling into the wrong hands and

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

Chapter 4 3 § HSLF-FS 2016: 40.

12

1 3 (15)

can affect patients' confidence in care. This in turn can affect

both the patients 'willingness to share data and the patients' willingness to provide

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

the authority for care and nursing analysis states 8 percent of

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

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

they considered it.28

It is therefore essential for health care to have one

competency structure based on well-implemented needs and

risk analyzes so that users are neither assigned too wide nor too narrow

privileges for accessing the journal systems.

Because a needs and risk analysis is a prescribed organizational measure

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

legal consequences if the data controller fails to implement

needs and risk analyzes.

In such a case, the person responsible for personal data has not used appropriate information

measures to restrict users 'access to patients' data in

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

fulfill their duties in health care. This contradicts as well

against the principle of data minimization under Article 5 (1) (c)

the Data Protection Regulation and the requirement to ensure adequate security for

personal data, including protection against unauthorized access or unauthorized use

treatment in accordance with Article 5 (1) (f), which is also stated in Article 32, which against ch.

Section 2 of the Patient Data Act and Chapter 4 Section 2 of the National Board of Health and Welfare's regulations.

Can the data controller not show that the provision on data minimization is complied with and that the data controller has taken measures to

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

personal data controller also did not fulfill the liability under Article

5.2 of the Data Protection Regulation.

When there has been a violation of the Data Protection Regulation

The Data Inspectorate a number of corrective powers available.29

The supervisory authority may, among other things, order the person responsible for personal data

to ensure that the processing takes place in accordance with the Regulation and if necessary

in a specific way and within a specific period.

Swedish Agency for Health and Care Analysis report For the sake of safety - The population

attitude to benefits and risks with digital health information 2017: 10 pp. 76-77

29 Article 58 (2) (a) to (j) of the Data Protection Regulation.

It follows from Article 58 (2) of the Data Protection Regulation that the supervisory authorities, in

Sweden Datainspektionen30, in accordance with Article 83 shall apply

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

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

the Data Protection Regulation are not insignificant and should be effective;

proportionate and dissuasive. A possible penalty fee can within

the area of care for the same violation result in completely different outcomes, depending on

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

Depending on whether the infringement concerns articles covered by Article 83 (4) or

83.5 of the Data Protection Ordinance, the penalty fees can be differently high. At
Violation of more central articles can penalize companies
amount to EUR 20 million or a maximum of 4% of the global
annual turnover during the previous financial 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 global annual sales during the previous one
financial year, depending on the maximum amount.
For authorities, national rules may state that authorities may be imposed
administrative sanction fees.31 According to ch. Section 2 of the Data Protection Act may
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
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, the higher scale of the penalty fees is actualised.32
Article 83 (2) of the Data Protection Ordinance sets out the factors that the Data Inspectorate must take into account when deciding on an administrative penalty fee
to be imposed, but also what is to affect the size of the penalty fee. Of
central to the assessment of the seriousness of an infringement is its nature,
degree of difficulty and duration as well as the degree of responsibility of the personal data controller (and the personal data assistant) taking into account the technical and
organizational measures implemented under the Data Protection Regulation.33

30
From 1 January 2021, the Data Inspectorate will change its name to
Integrity 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.

14

1 5 (15)

In the case of a minor infringement, the supervisory authority may issue one

reprimand instead of imposing a penalty fee.34 Not implementing one

needs and risk analysis prior to the allocation of authorizations does not constitute a minor

violation.

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

the person responsible for personal data makes a needs and risk analysis before allocating

permissions occur. This is a matter of sensitive personal data, often large

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

fundamental freedoms and rights of data were unauthorizedly disclosed

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

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

usually that a penalty fee should be paid.

34

Recital 148 of the Data Protection Regulation.

15