

Guidance on impact assessment

A practical guide

February 2025



IMY. Guidance on impact assessment - A practical guide. If you have any questions about the content, please contact the Swedish Authority for Privacy Protection, telephone 08-657 61 00, e-mail imy@imy.se, or visit www.imy.se

Contents

About the guide	5
What is an impact assessment?	6
IMY proposal– a documented ten-step process	10
Step 1. Assess the need to carry out an impact assessment	12
1.1 The obligation to carry out an impact assessment.....	13
1.2 No obligation to carry out an impact assessment	15
Step 2. Set up a working group and plan the work	16
Step 3. Make a systematic description of the personal data processing	18
3.1 Nature of the treatment	19
3.2 Scope of the treatment	22
3.3 The context of treatment.....	22
3.4 Purpose of the treatment.....	22
3.5 Necessary resources.....	22
3.6 Functional description of the treatment.....	23
3.7 Roles and responsibilities	23
Step 4. Carry out a legal analysis	24
4.1 Existing regulations	25
4.2 Ensure compliance with data protection principles and legal basis for processing.....	25
4.3 Ensure that data subjects' rights can be enforced.....	32
4.4 Safeguards for international transfers	34
4.5 Make an overall assessment	34
Step 5. Managing risks: identifying, analyzing and addressing risks	35
5.1 Identifying the risks.....	37
5.2 Analyzing the risks.....	39
5.3 Addressing the risks	41
5.4 Follow up and reassess risks.....	44
Step 6. Request prior consultation with IMY if risk remains high	45
Step 7. Collect feedback from stakeholders	47
7.1 Recommendations from the Data Protection Officer.....	48
7.2 Comments from registrants	48
7.3 Comments from other stakeholders.....	50
Step 8. Make an overall assessment	51
Step 9. Embedding the assessment in the organization	53
Step 10. Follow up the impact assessment continuously	55
Sources	57



About the guide

IMY's guidance on impact assessment is aimed at organizations that process personal data under the Data Protection Regulation ¹ and who want support in conducting impact assessments. The purpose of the guide is to facilitate the work with impact assessments and reduce uncertainty about how the various steps are carried out and how the regulations should be understood.

In **A Practical Guide**, IMY suggests how to carry out an acceptable impact assessment. It can be read separately or together with the two supporting templates developed by IMY. To facilitate the planning of the practical work, and to be able to adapt the approach to the treatment in question, we recommend that you read the guide in full before starting the impact assessment. The guide is designed primarily for those who have little or no knowledge of impact assessments.

In the annex **Legal interpretation support**, IMY goes through the regulations in the area and the interpretation support for this. The annex is designed for those who want to have the legal interpretation support together and in-depth information on how the regulations should be understood.



IMY guidance on impact assessment

A practical guide
Annex Legal interpretative support



Templates to support your work

IMY template for Assessing the need for an impact assessment
IMY template for Impact assessment under the GDPR
Excel sheet Risk management in impact assessment



IMY website

All materials related to the practical guide can be found at imy.se/impactassessment

Our website www.imy.se provides general information on impact assessments.

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

What is an impact assessment?

A DPIA is an ongoing and documented process that helps data controllers² to comply with the GDPR for high-risk processing operations. The process provides an in-depth understanding

for the processing in question, the risks it poses to the rights and freedoms of individuals, and the security and protection measures required to mitigate those risks.

An ongoing and documented process

One of the purposes of the GDPR is to protect the fundamental rights and freedoms of individuals - and in particular their right to the protection of their personal data.⁽³⁾ In order to guarantee the rights of individuals, the GDPR places a strong responsibility on those who collect and process personal data to ensure that the processing with the applicable rules. This applies in particular to so-called *high-risk processing*, i.e. processing of personal data that is deemed likely to result in a high risk to the rights and freedoms of individuals. The high risks may be due, for example, to the processing of sensitive personal data, the introduction of new technologies for data processing or the processing of personal data through extensive surveillance.

It is important to be aware that impact assessment is an ongoing process. It is not a one-off activity with a clear end. This means that the impact assessment should be updated and reassessed on an ongoing basis⁽⁴⁾.

An obligation under existing legislation

Provisions on data protection impact assessment are contained in Article 35 of the GDPR. According to the first paragraph of the Article, controllers shall carry out a DPIA for "processing operations" likely to result in a high risk to the rights and freedoms of natural persons.

2 A *controller* is a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data (see Article 4(7) of the GDPR). The decisive factor in determining who is the controller is the person or persons who have determined the purposes of processing and exercise influence over the personal data collected and processed, the period for which they are stored and who has access to them. The assessment of who is the controller or processors for a particular processing operation should always be based on the factual circumstances of the specific case (see EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, version 2.1, pp. 3 and 9 et seq.)

3 The right to the protection of personal data is enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (2012/C 326/02).

4 Article 35(11) of the GDPR.

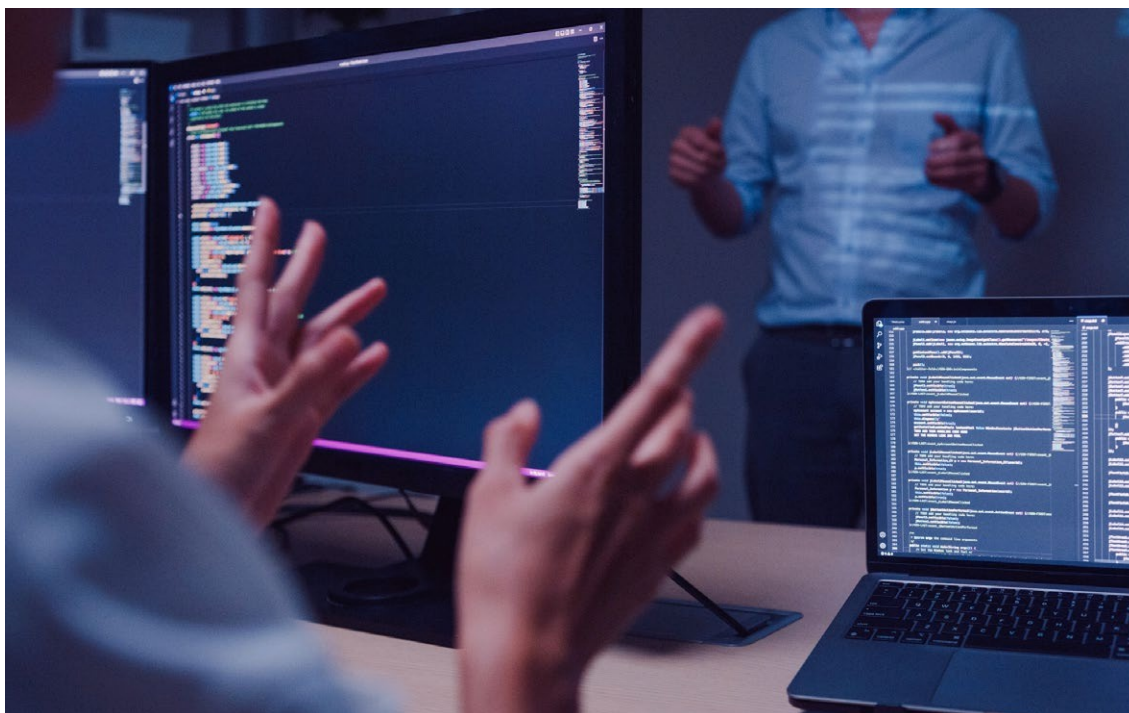
The GDPR requires controllers to take a risk-based approach to ensuring compliance with its provisions and to adapt data protection to the risk level of the processing. The higher the risk, the more far-reaching the security measures, active data protection work and more frequent monitoring are required. Simply put, *high-risk processing operations* entail more obligations for controllers, and conducting impact assessments is one of them.

A practical tool to ensure compliance applicable regulations

Properly implemented, a DPIA is a useful tool for data controllers to assess risks and ensure compliance with the provisions of the GDPR. The DPIA can be used to get a holistic view of the processing of personal data and its consequences, and to minimize the processing so that it does not become unnecessarily extensive in relation to its purpose⁽⁵⁾.

The DPIA also creates the conditions for controllers to meet the requirement of data protection by design.⁽⁶⁾ In addition, it is on the basis of the DPIA that controllers should determine whether there is an obligation to request prior consultation with the supervisory authority.⁽⁷⁾

A well-conducted and documented impact assessment is an important part of fulfilling the principle of accountability⁽⁸⁾.



5 See the data minimization principle in Article 5(1)(c) of the GDPR.

6 See Article 25 of the Data Protection Regulation.

7 See Article 36 of the GDPR. Prior consultation must be requested if the impact assessment shows that the processing would result in a high risk, also taking into account the risk mitigation measures envisaged.

8 *The principle of accountability* imposes an obligation on controllers to comply with the provisions of the GDPR and is expressed in Article 5(2) of the GDPR. Controllers must be responsible for compliance with all the principles governing the processing of personal data and be able to demonstrate this. Controllers are also responsible for implementing appropriate technical and organizational measures and ensuring a level of security appropriate the risk to the rights and freedoms of natural persons posed by the processing (see Article 32 of the GDPR).



An impact assessment shall include at least:

- a systematic description of the intended processing of personal data and its purposes
- an assessment of the need for the processing of personal data and whether the intrusion is to the purposes of the processing
- an assessment of the risks to the rights and freedoms of natural persons
- the measures planned to manage the risks and demonstrate compliance with the GDPR⁹



A DPIA requires the controller to:

- consult the Data Protection Officer (if appointed)¹⁰
- check that the processing complies with any codes of conduct approved in the relevant industry¹¹
- seek the views of data subjects¹² or their representatives, where appropriate¹³
- conduct a review to assess whether the processing is carried out in accordance with the impact assessment, if necessary¹⁴

9 Article 35(7) of the GDPR.

10 Article 35(2) of the GDPR.

11 Article 35(8) of the GDPR with reference to Article 40 of the GDPR. A code of conduct is a kind of rulebook on the processing of personal data developed by and voluntarily applied in, for example, a particular industry or sector.

12 The term data subject can be defined as the person whose personal data is being processed, cf. Article 4(1) of the GDPR.

13 Article 35(9) of the GDPR.

14 Article 35(11) of the GDPR.

About the practical guide

IMY's guide to practical work on DPIAs is based on the criteria for acceptable DPIAs set out in Annex 2 of the European Data Protection Board (EDPB) Guidelines on DPIAs¹⁵. These criteria clarify and develop the minimum requirements under Article 35 of the GDPR¹⁶

It is natural that the design of impact assessments will vary in scope and detail depending on, among other things, the complexity of the treatment to be assessed and the size of the individual organization. The approach described in the IMY Guide should be seen as a point. The approach may need to be adapted according to the resources and competences available. The steps may also need to be implemented in a different order than described in the guide. For example, depending on the processing in question, the views of data subjects may in some cases need to be sought at an earlier stage than indicated in the guide. Where the controller has appointed a DPO, IMY believes that the DPO should be consulted on an ongoing basis, and not only in the context of collecting feedback from stakeholders.

The controller must document the assessments made and the decisions taken in the context of the impact assessment. The impact assessment must be documented in order for the organization to demonstrate compliance with the GDPR.¹⁷ However, the controller has the discretion to determine the scope and level of detail of the documentation.



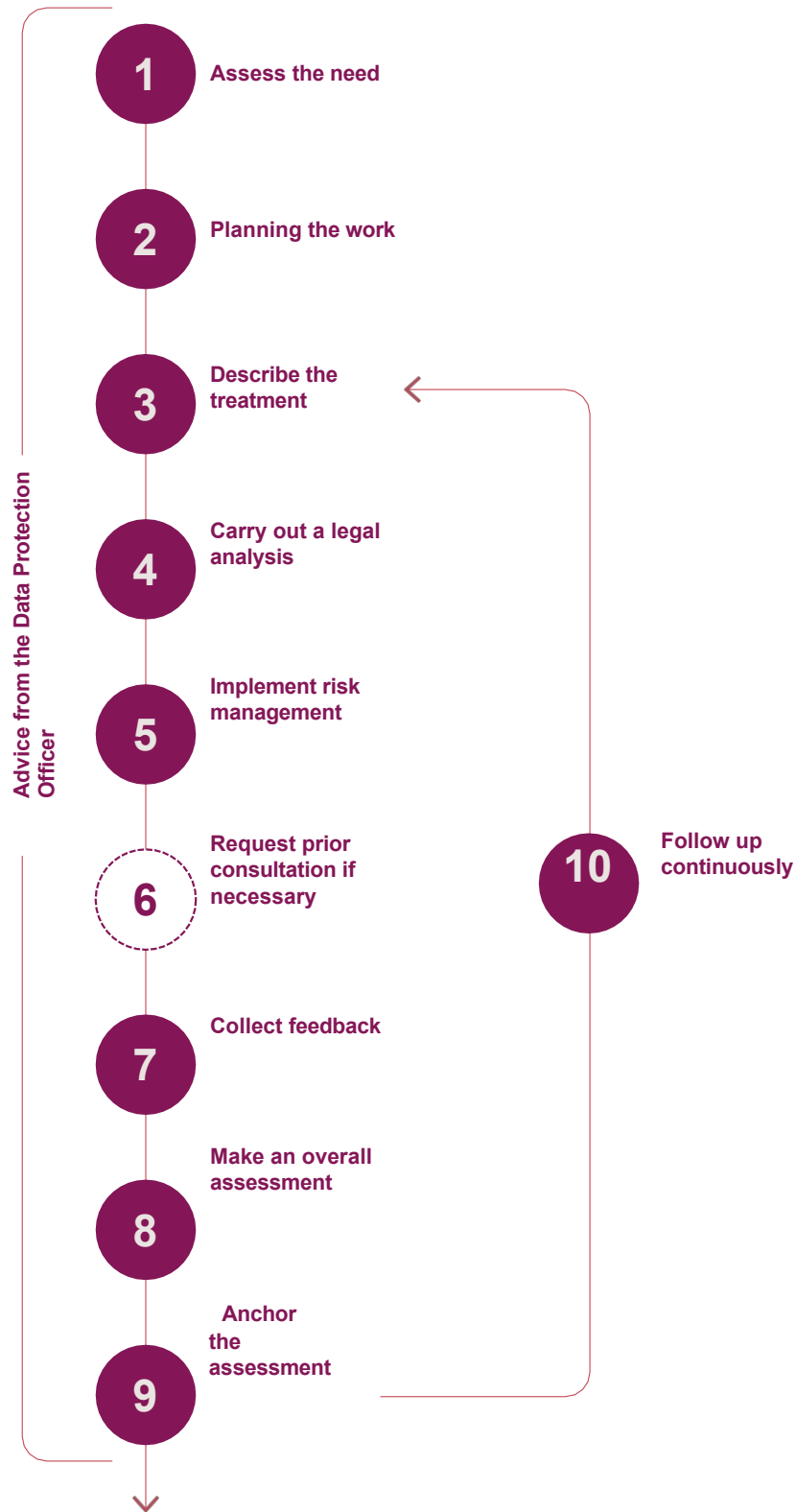
¹⁵ Article 29 Working Party *Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" within the meaning of Regulation 2016/679* (WP 248 rev. 01). The EDPB has endorsed the guidelines, Endorsement 1/2018.

¹⁶ See WP 248, pp. 19 and 22.

¹⁷ Article 5(2) of the GDPR (accountability principle).

The IMY proposal – a documented 10-step process





Step 1.

Assess the need
to carry out an
impact
assessment



Controllers may consider processing personal data for a variety of reasons, such as a development project, a new business process or the purchase of a new business system. It will then be necessary to assess whether an impact assessment needs to be carried out. If the controller has appointed a DPO, the DPO should always be consulted on the need to carry out a DPIA.

IMY has developed a template to assess the need to conduct a DPIA. The template is designed to make it easier for controllers to document this in a structured way.



Template to support your work

IMY's template for Assessing the need for a DPIA under the GDPR

All materials related to the practical guide can be found at imy.se/impactassessment

1.1 The obligation to carry out a impact assessment

A DPIA shall be carried out if a *type of processing*, in particular with the use of new technologies and taking into account its nature, scope, context and purposes, is likely to result in a high risk to the rights and freedoms of natural persons.¹⁸ The fact that it is *the type of processing* that is at stake when assessing need for a DPIA means that measures that can reduce or eliminate risks of the individual processing envisaged shall not be considered at this stage.

As a general rule, the impact assessment should be carried out before the processing starts. However, an impact assessment may also need to be carried out if the controller takes decisions that change the risks of an ongoing processing operation.

That is, if it becomes a *type of processing* likely to result in a high risk to the rights and freedoms of natural persons.

¹⁸ Article 35(1) of the GDPR.

Support in assessing whether there is a need for impact assessment

When assessing whether a DPIA is mandatory, the controller shall rely on the following sources of law:

1 The factors listed in Article 35(1) of the GDPR.

Article 35(1) mentions certain factors to be taken into account when you assess whether an impact assessment needs to be carried out. They are

- use of new technologies
- the nature of the treatment
- the scope of the treatment
- the context of treatment
- the purpose of the processing.

2 The examples given in Article 35(3) of the Data Protection Regulation.

The examples mentioned are:

Regulation.

- A systematic and comprehensive assessment of personal aspects relating to natural persons, based on automated processing, including profiling, on which decisions are based that produce legal effects concerning natural persons or similarly significantly affect natural persons.
- processing on a large scale of special categories of data, as referred to in Article 9(1), or of personal data relating to criminal convictions and offences involving criminal offences, as referred to in Article 10.
- Systematic monitoring of a public place on a large scale.

3 IMY's list under Article 35.4 of the GDPR.

The list complements the examples given in Article 35(3) of the GDPR and is based on the criteria set out in the EDPB Guidelines on Impact Assessment.

As a general rule, an impact assessment should be carried out if the envisaged personal data processing operation meets at least two of the nine criteria in the IMY list. The list is not exhaustive. A DPIA may need to be carried out in an individual case even if only one of the criteria in the list is met.



In-depth information

Legal Interpretative Support Annex: Section 4. Support in assessing whether to carry out an impact assessment
 IMY's list under Article 35(4) of the GDPR

All materials related to the practical guide can be found at imy.se/impactassessment



Read more about the obligation to carry out impact assessments in individual areas

IMY website IMY.se– [Impact assessment - personal data at work](#) IMY website IMY.se - [Impact assessment for camera surveillance](#)

1.2 No obligation to carry out a impact assessment

The controller is not obliged to carry out a DPIA when:

- **It is not a "type of processing" likely to result in a high risk to the rights and freedoms of natural persons.**

For most processing operations of personal data, a DPIA is not required. However, controllers must continuously analyze the risks arising from their processing operations in order to be aware of whether a processing operation becomes a "type of processing" for which a DPIA must be carried out.

- **It is a treatment very similar to a treatment for an impact assessment has already been carried out.**

For a previously conducted DPIA to be used for a new, planned processing operation, the processing operations must be similar in nature, scope, context, purposes and risks. The possibility of conducting a DPIA for several processing operations also means that several controllers can conduct a joint DPIA for different processing operations, as long as the envisaged processing operations are sufficiently similar⁽¹⁹⁾.

In general, for a single DPIA to be sufficient, the processing operations must be very similar. The controller must be able to justify that the envisaged processing is sufficiently similar to the previous or joint processing.

- **A general impact assessment has been carried out in the context of the legislative process.**

The legislator can carry out a general impact assessment as part of the drafting process to make it easier for the controllers concerned (e.g. the authorities or other actors who are assigned tasks under the new legislation).²⁰ However, drafting processes rarely carry out comprehensive impact assessment required by the GDPR, which means that the controller often has to supplement this with its own impact assessment of the practical, technical and organizational conditions for processing.²¹



In-depth information

Annex Legal interpretative support: Section 4.4. No obligation to carry out an impact assessment

All materials related to the practical guide can be found at imy.se/impactassessment

¹⁹ See Article 35(1) of the GDPR.

²⁰ Article 35(10) of the GDPR. See recital 93 of the GDPR.

²¹ See e.g. IMY's consultation response of September 14, 2023 in IMY-2023-8865; Bill 2021/22:177, Coherent health and care documentation, p. 54; SOU 2024:33, Shared health data - double benefit, p. 320 f.

Step 2.

Set up a working group and plan the work



Once the controller has decided to carry out an impact assessment, the next step is to plan its implementation and determine the resources needed.

For larger organizations, it is advisable to set up a working group composed of people who have knowledge of:

- the information to be processed (e.g. an employee who will work in the process or with the system where the data will be processed)
- how the processing will be carried out technically (e.g. an IT technician)
- information security and risk management (e.g. corporate information security officers)
- data protection legislation (e.g. a data protection lawyer).

Smaller organizations rarely have all these competences in place, and sometimes the same person may therefore need to play several roles. To ensure that different perspectives are taken into account

it is often preferable to involve several people with different skills in carrying out the impact assessment.

To facilitate the work on the DPIA, the data controller should appoint a person in the working group who is responsible for coordinating and driving the implementation process forward. In many organizations, the DPO is the person most knowledgeable about DPIAs and the applicable regulation. However, it is important that the controller organization understands that it is not the DPO who should be responsible for carrying out the impact assessment.

Already at the initial stage of the process, the controller should also identify who (person and function) is competent to decide on or adopt the impact assessment.

A timetable for the work should then be established. Remember to set aside time to anchor the impact assessment with management and the DPO, and– when appropriate - to collect data subjects' views.



In-depth information

Annex Legal Interpretative Support: Section 6. The role of the DPO in the impact assessment

All materials related to the practical guide can be found at imy.se/impactassessment

Step 3.

Make a systematic description of the personal data processing



The systematic description of the processing and its purposes ²² means that the description should be done in a thorough and methodical manner. It is important that the description of the processing is clear, and as comprehensive as possible, to enable the controller to have a complete overview of the processing.

The description should serve as a basis for further work on the impact assessment. When assessing what is relevant to describe in each part, you should bear in mind that it is the impact of the processing on the rights and freedoms of individuals that should be assessed within the framework of the impact assessment.

The following should be included in the systematic description:

- **the nature of the treatment** (see section 3.1)
- **the scope of the treatment** (see section 3.2)
- **the context of the treatment** (see section 3.3)
- **the purposes of the processing** (see section 3.4)
- **necessary resources** (see section 3.5)
- **functional description of the treatment** (see section 3.6)
- **roles and responsibilities** (see section 3.7).

3.1 Nature of the treatment

General description and background

When describing personal data processing, it is useful to start by defining and delimiting the object of the impact assessment, i.e. the product, service, software or process in question. This provides a framework for the more detailed description of the processing to be made later and clarifies the context of the processing. The initial description may also include a background to why the processing is being planned (for example, that there has been a business change or a change in the law). If a complex system is being implemented, it is sometimes the case that several different types of processing operations are carried out in the same system. In such cases, it is often appropriate to split the description into several parts.

The need to carry out an impact assessment is sometimes identified in the context of a needs analysis, pre-procurement study, process mapping, information classification or a risk analysis. Documentation from such work is often useful when describing the processing. However, it is important to remember that the description should enable the readers - i.e. the data subjects, the organization's management, the DPO, the supervisory authority and other stakeholders - to understand the processing operations, what they entail and their purposes. Therefore, it is not sufficient to simply refer to other documentation to meet the requirement of a systematic description.

²² The requirement for systematic description is set out in Article 35(7)(a) of the GDPR.

Categories of personal data

It is very important to identify and describe the types of personal data that will be processed. Examples of types of personal data could be data on

- age
- queue
- education and training
- salary
- images of people
- audio recording of voices.

It is not always clear what constitutes personal data. Remember that technical data (e.g. IP addresses), tracking data (e.g. cookies) or car registration numbers can also be personal data.



Read more

IMY website imy.se – [Personal data](#)

Special categories of personal data ("sensitive personal data")

There are categories of personal data that are considered particularly sensitive. These include data revealing "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and data concerning health, a person's sex life or sexual orientation, genetic data and biometric data for the purpose of uniquely identifying a person"⁽²³⁾.

As a general rule, the processing of such personal data is prohibited.²⁴ However, there are exceptions. If the intended processing involves sensitive personal data, it must be ensured that one of the GDPR exemptions applies in order for the processing to be allowed.²⁵

Sometimes, the processing of such data needs to be supported by complementary national law, EU law or collective agreements in order to be allowed.

Where appropriate, the impact assessment should describe the legal basis for processing special categories of personal data.



Read more

IMY website imy.se – [Sensitive personal data](#)

23 Article 9(1) of the GDPR.

24 Article 9(1) of the GDPR.

25 The exceptions are set out in Article 9(2) of the GDPR.

Personal data relating to breaches of the law

According to the GDPR, personal data relating to criminal convictions and offences involving criminal offences may only be processed under the "control of a public authority" or if there is a legal basis for the processing.²⁶ If the controller is not a public authority and this type of data is included in the envisaged processing, the controller should carefully ensure and specify the legal basis.



Read more

IMY website imy.se – [Personal data on breaches of law](#)

Personal data requiring special protection

Some personal data are considered to be worthy of special protection even though they do not belong to any of the above categories. Personal data concerning children and social security numbers are examples of personal data requiring special protection. It is therefore important to pay attention to whether such data will be processed, and if so, to estimate the amount of such personal data (e.g. what proportion relates to children).



²⁶ Article 10 of the Data Protection Regulation.

Categories of registrants

The description should indicate which categories of data subjects will be covered by the processing, for example "employees" or "customers". If the data subjects are in some form of dependency relationship with the controller (e.g. employees, patients or pupils), this should be indicated. It should also be indicated whether any of the categories include children or other particularly vulnerable groups, such as the elderly or people with disabilities.

3.2 Scope of the treatment

It is important to estimate the expected scope of the processing in terms of the number of individuals concerned and the amount of personal data. The number of different categories of personal data is also relevant. If it is difficult to assess this (for example, because of uncertainty about the level of interest in the product), the controller should allow for different scenarios in its description. The scope of the processing is generally of great importance in the assessment and management of risks to be implemented later. The geographical scope of the processing, i.e. the countries in which the data will be processed and whether they are outside the EU/EEA, should also be indicated.

3.3 The context of treatment

Describing the context of treatment means describing the treatment from a broader perspective, taking into account various internal and external factors.

This may include, for example

- previous experience with similar treatments or lack thereof
- the business has experienced problems with similar treatments in the past
- the treatment is innovative in some way
- the treatment may be questioned or perceived as unpredictable
- the extent to which individuals will have control over their personal data
- relevant codes of conduct or other certification schemes.

3.4 Purpose of the treatment

It is essential that the processing of personal data has one or more clearly defined purposes. The controller needs to be absolutely clear about what is to be achieved by the intended processing and be able to specify this. If there are several purposes, it is important to distinguish between them. A detailed description in this part is important in order to be able to later assess whether the processing meets the GDPR requirements of necessity and proportionality.

3.5 Necessary resources

The controller needs to identify which resources are necessary to carry out the planned processing. This will facilitate future work to identify the potential risks associated with each resource. For example, software, servers, hardware, networks, cloud services, etc.

3.6 Functional description of the treatment

In the functional description, the controller should describe how the processing takes place in more detail. In this part, a flowchart can help to explain how the personal data "moves". Such a diagram is also useful later in the impact assessment when identifying risks.

The functional description should indicate how the personal data is to be collected and where it comes from (for example, whether it comes directly from the data subject via questionnaires, web forms or interviews, or whether they are to be collected without the knowledge of the data subject via public data collections or databases). It should be made clear how the data will be recorded and transmitted (e.g. whether paper questionnaires will be sent to a data collection center or whether any data will be provided by telephone or any digital tool). It should also be clarified which systems will be used in the different stages of the processing, how long the personal data will be stored and the procedures for deletion or anonymization.

It is important to justify the retention period and explain the reasons for it (e.g. legal or specific business requirements). If it is not possible to set an explicit end time for a processing operation (e.g. two years from registration), the duration of the processing operation should be expressed in some other way that can be followed up by the controller.

3.7 Roles and responsibilities

Personal data liability

Sometimes several controllers may be involved in the same processing operation. In such cases, it is very important to clarify the division of responsibilities before the processing starts. Carefully specify the controller(s), i.e. the actors who alone or jointly determine the purposes and means of the processing of personal data.²⁷ Indicate whether the processing involves a joint controller with another actor or whether one of the actors will be a processor. The division of responsibilities should be carefully documented.

Recipients including data processors

Often there is a need to share the personal data with different recipients. The description of the processing should include information on who will receive the personal data in the course of the planned processing (e.g. IT suppliers or other companies within the same group).

The impact assessment should indicate whether processors will be involved in the processing, and if so, their identity (including organization number and address of the place of business), the services performed by the processor and the country where the processor processes the data.



Read more

IMY's website imy.se – [Controllers and processors](#)

²⁷ See Article 4(7) of the GDPR.

Step 4. Carry out a legal analysis



The next step is to assess whether the legal conditions for carrying out the processing are met. This gives a good indication of how necessary and proportionate the processing is in relation to its purposes. If the envisaged processing is not in line with the applicable data protection legislation (for example, because it lacks a legal basis), it is unlawful and cannot be carried out. An impact assessment cannot change this. Therefore, if the processing is unlawful, there is no reason to proceed to the next step in the impact assessment.

4.1 Existing regulations

Start by summarizing the current regulatory framework. Beyond the General Data Protection Regulation and the Data Protection Act⁽²⁸⁾, for example, marketing laws and government-specific registry legislation may be relevant. Adopted codes of conduct, completed certifications and industry practices should also be identified.



Read more

IMY's website imy.se – [How the laws fit together](#)

IMY's website imy.se – [Code of Conduct under GDPR](#)

4.2 Ensure compliance with data protection principles and that there is a legal basis for processing

According to the GDPR, the following basic principles apply to the processing of personal data:

- **legality, regularity and transparency** (Article 5(1)(a))
- **purpose limitation** (Article 5(1)(b))
- **data minimization** (Article 5(1)(c))
- **accuracy** (Article 5(1)(d))
- **storage minimization** (Article 5(1)(e))
- **privacy and confidentiality** (Article 5(1)(f)).

The impact assessment should describe how the envisaged processing complies with these principles. Compliance with the fundamental principles of data protection is a key element in ensuring that processing is necessary and proportionate.

28 Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation.

The principle legality, regularity and transparency

Legality

In order to comply with the principle of lawfulness, the provisions of the GDPR and other complementary legislation must be respected.

A prerequisite for the lawfulness of the processing of personal data is that it is supported by a legal basis.²⁹ There are six legal bases:

- consent
- legal obligation
- contract
- protection of fundamental interests
- exercise of public authority and public interest
- balancing of interests.

The legal basis (or bases) for the processing in question should be clearly stated in the impact assessment. Sometimes a processing operation may be supported by more than one legal basis, in which case it is important to be clear which legal basis is being used in the particular case. It may also be the case that different parts of the processing are to be supported by different grounds, which also needs to be clarified. The validity and reasonableness of the legal basis must be justified. If the legal basis is balancing of interests⁽³⁰⁾, an assessment of the balancing of interests must also be documented.



²⁹ Article 6(1)(a) to (f) of the GDPR.

³⁰ Article 6(1)(f) of the GDPR.

Legal basis required for processing personal data

Consent (Article 6(1)(a))

If consent is considered as a legal basis, the controller shall take into account the conditions for consent set out in Article 7 of the GDPR, which means *inter alia* that:

- The data subject's consent must be a freely given, specific, informed and unambiguous indication of his or her wishes within the meaning of the GDPR.
- The controller must be able to demonstrate that the data subject has consented to the processing of their personal data.
- The data subject has the right to withdraw consent at any time, and that withdrawing consent should be as easy as giving it.
- The consent must be in accordance with the requirements of the GDPR.

Contracts (Article 6(1)(b))

In order for this basis to be used, the data subject must be or become a party to the contract.

Legal obligation (Article 6(1)(c))

In order for a legal obligation to provide a legal basis for the processing of personal data, it must be established in accordance with Union law or the national law of a Member State. A legal obligation under Swedish law may result from a law or other statute, from a collective agreement or from a decision made on the basis of a law or other statute. It is important to bear in mind that the purpose of the processing must also be stated in the relevant obligation.

Protection of fundamental interests (Article 6(1)(d))

This legal basis is very rarely invoked. It is mainly applicable when people's lives or health are at stake and is sometimes used in healthcare.

Exercise of official authority and public interest (Article 6(1)(e))

In addition to public authorities and other public bodies performing tasks in the public interest in the sense referred to, private actors carrying out, for example, healthcare or education activities may be covered. For a task in the public interest to provide a legal basis for processing personal data, it must be established in accordance with Union or Member State law.

Balancing of interests (Article 6(1)(f))

For a balancing of interests to provide a legal basis for processing personal data, three conditions must be met. The controller must be able to demonstrate 1) there is a legitimate interest, 2) the processing of personal data in question is necessary to achieve that interest, and 3) the legitimate interest outweighs the interests or fundamental rights or freedoms of the data subjects.

Correctness

In general terms, *the fair* processing of personal data means that the processing must be fair, reasonable and proportionate in relation to the data subjects.

Fairness means that personal data must be processed in a way that the data subject can understand, and that it must not be discriminatory.

The processing of personal data must be proportionate to the benefits it brings. The controller therefore needs to balance its own interests against those of the data subjects. The assessment is also influenced by what processing of personal data the data subjects can reasonably expect. The processing of personal data must be intelligible to data subjects and not carried out in a covert or manipulative manner.

Transparency

The *transparency* requirement means that it must be clear to data subjects that and how their personal data are processed. Data subjects must have the opportunity to know why their personal data is processed, how it is collected and how it is used. Data subjects should also be informed of their rights (for example, how to have inaccurate data rectified and how to have personal data deleted). Information on the processing of personal data should be easy to find and should be formulated in a way that is simple and understandable for data subjects. It is particularly important to use clear and plain language when the data subjects are children.

□ — Example of questions to check compliance with the principle:

□ — *Legality*

- Does the activity comply with the provisions of the applicable legislation?
- Is there a legal basis for the processing?
- If the legal basis is balancing of interests, has the balancing of interests been documented?
- If the legal basis is consent, is the consent voluntary, specific, informed and unambiguous within the meaning of the GDPR?
- If the legal basis is consent, can consent be withdrawn?

Correctness

- Is the processing carried out in a way that the data subject can reasonably expect?

Transparency

- How are data subjects informed about the processing of personal data?
- Is the information easily accessible to data subjects?
- Is the information adapted to the target audience (e.g. children)?
- Are there procedures in place to update the information?

**Read more**IMY website imy.se – [Legal basis for processing personal data](#)

The principle of purpose limitation

The purpose limitation principle means that personal data must be collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes. The purpose must be defined before the processing starts and must be precisely specified. The purpose of the processing is crucial for assessing which data are necessary to process, the legal basis on which the processing can be supported and for complying with other fundamental data protection principles.

The data subject should be able to understand from the description of the purpose why and how the personal data will be used. It is important to be aware that the purpose cannot be changed once the processing has started and the data subjects have been informed of the purpose of the processing. Personal data that has been for one purpose cannot be processed later for another purpose that is incompatible with the original one. It is important to have procedures and other measures in place to ensure this.

**Examples of questions to check compliance with the purpose limitation principle**

- Has the purpose(s) been documented and how?
- Is the purpose described in such a concrete and specific way that it is easy to establish that the processing is compatible with it?
- Has the processing of the data for purposes other than those specified been restricted by, for example, contractual clauses, guidelines or other security measures?

The principle of data minimization

The principle of data minimization means that the personal data processed should be adequate, relevant and not excessive in relation to the purposes for which they are processed. Describe how (through which measures) it will be ensured that only personal data necessary for the purpose will be processed. It should also indicate that the controller has considered whether there are alternative ways of carrying out the processing which are equally effective in achieving the purpose, but which interfere less with the fundamental rights and freedoms of individuals (for example, by entailing limited data collection or requiring less detailed information).

If the purpose can be achieved without processing certain data, the processing those particular personal data is not necessary and shall not be carried out.

Examples of questions to check compliance with the data minimization principle

- Is it clear why the personal data to be processed is needed to fulfill the purpose of the processing in question?
- Have you checked that no data is collected just "because it might be useful to have"?
- Free text fields in forms: Is it necessary to use them? Are there clear instructions on what should be entered in the free text fields (to prevent the collection of unnecessary data)? Is it clear which fields are optional and which are mandatory? Are the optional fields really necessary to achieve the purpose of the processing?
- Camera surveillance: Is it necessary to collect data from the entire camera footprint or should some parts be digitally masked?

The principle of accuracy

Personal data processed must be accurate and (where necessary) kept up to date. If the personal data is inaccurate, it should be corrected or deleted. It is therefore important that procedures are in place to detect errors and to correct and delete inaccurate personal data when requested by data subjects.

Examples of questions to check compliance with the principle of accuracy:

- Is the data static or does it require updates?
- How is it ensured that incorrect data is corrected?
- How often should the accuracy of the data be checked?
- Can the data subject influence the accuracy of the data and update it if necessary?
- How is the accuracy of data received from another activity ensured?
- How is it ensured that the data collected concerns the right person?

The principle of storage minimization

The principle of storage minimization means that personal data must not be kept in a form which permits identification of the data subject for longer than is necessary for the purposes for which the personal data are processed. The planned storage period should therefore be justified on the basis of what is necessary for the purpose of the processing. Since what is necessary is not always proportionate, proportionality also needs to be justified. It is important that there are procedures for the deletion of personal data.



Examples of questions to check compliance with the principle storage minimization:

- For what purposes and for how long the data be processed?
- Will the data be deleted when it is no longer needed and how will this happen in practice?
- Are there legal requirements determining the retention period of the personal data processed?
- Will it be possible to use automatic deletion of data once the retention period has expired, or should the data be deleted manually?
- If erasure is not appropriate, will the personal data be anonymized?

The principle privacy and confidentiality


The controller shall implement appropriate technical and organizational measures to ensure the integrity and confidentiality of personal data.

Integrity is about ensuring that data remain unchanged during processing, transmission and storage. Personal data must therefore be protected against unauthorized loss, destruction or deliberate or accidental alteration. Confidentiality means that personal data shall be accessible only to those who, by reason of their duties, and are entitled to have access to it. Personal data shall be protected so that it cannot be read or otherwise processed by unauthorized persons.



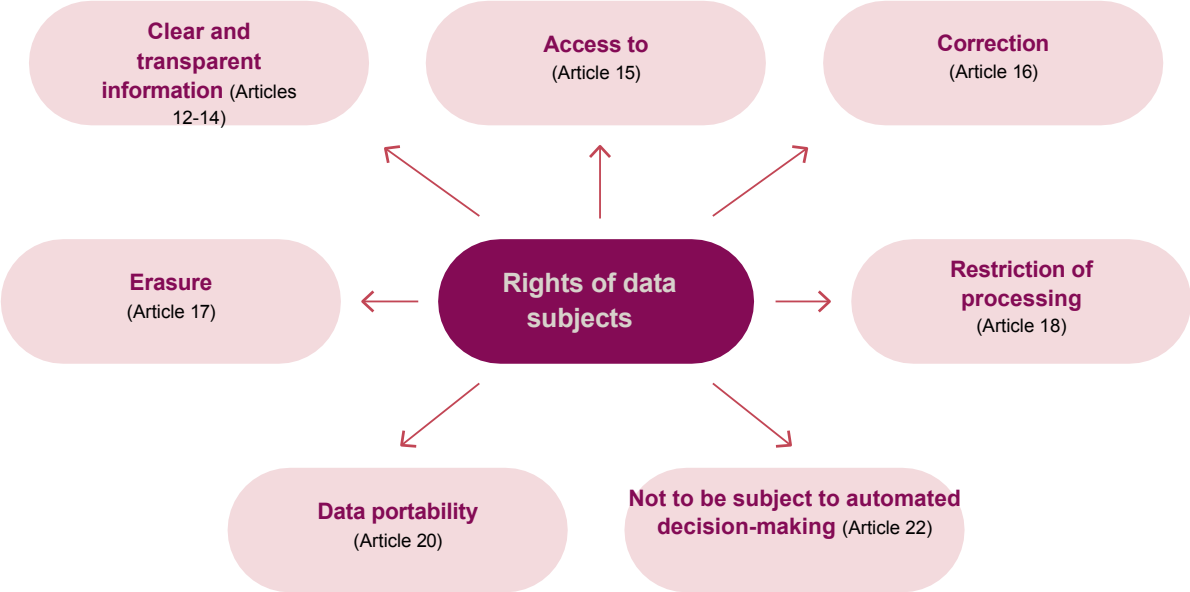
Example of questions to check compliance with the principle:

- Integrity**
 - Are there policies or procedures on how data can be changed and by whom?
 - Are backups made and what the procedures for doing so?
 - Is logging done when data changes?
- Confidentiality**
 - Are procedures and measures for access control?
 - Are there applicable confidentiality provisions for the data?
 - Do the people who will handle the data have a sufficient understanding of confidentiality and privacy?

 **Read more**
IMY website imy.se – [Basic principles under GDPR](#)

4.3 Ensure that data subjects' rights can be enforced

Data subjects have a number of rights set out in Chapter III of the GDPR. The controller needs to ensure that these rights will be able to be met during processing. The data subject has (with some exceptions) the right to:





Examples of questions to check that data subjects' rights can be met:

- How are data subjects helped to exercise their rights under the GDPR?
- Is there a form or other contact channel for data subjects to exercise their rights?
- Is the information easy to find for data subjects?
- Is there a process to handle data subjects' requests?
- Is there a person responsible for ensuring that the rights of data subjects are respected?
- Do data subjects receive clear and sufficient information about the processing of their personal data?
- Can all data relating to data subjects be compiled?
- Can a copy of the data subjects' data be easily obtained?
- Is it possible to provide the data in electronic form if requested by the data subjects?
- How does the procedure for deleting personal data work if data subjects withdraw their consent to processing?
- How is the data deleted in practice (manual or automated deletion)?
- Are there any obstacles to the deletion (such as legal retention periods or similar)?
- How is the right to data portability exercised in practice? Is it technically possible?
- Does the processing of personal data involve automated decision-making which significantly affects the data subject? If yes, what is this based on?



Read more

IMY website imy.se - [Data subjects' rights](#)

4.4 Safeguard measures for international transfers

Personal data may only be transferred to a country outside the EU/EEA, a so-called third country, under certain conditions. In order for such a third country transfer to be allowed, the controller must ensure an adequate level of protection of the rights and freedoms of natural persons.³¹ Examples of safeguards that may allow the third country transfer are binding corporate rules, standard contractual clauses or an adequacy decision by the European Commission.

If personal data will be transferred to a third country, the controller must be able to demonstrate the lawfulness of the transfer.



Read more

IMY website imy.se – [Transfer of personal data to third countries](#)

4.5 Make an overall assessment

Before starting the risk management, an overall assessment of the legal analysis should be made. Document the assessment of whether the processing is necessary and proportionate in relation to its purposes. The overall assessment in step 4 should lead to a decision on whether the processing, in the form envisaged, meets the legal requirements of the GDPR and supplementary legislation. If the processing does not meet the legal requirements, the processing should not be carried out as planned.

Note that an overall assessment of the necessity and proportionality of the processing in relation to the purposes should also be made after the risk management has been carried out and relevant comments have been (see step 8). This is to ensure that the benefits of the processing are proportionate to the risks to individuals' rights and freedoms that have been identified.

³¹ The provisions on the transfer of personal data to third countries or international organizations are set out in Chapter V of the GDPR.

Step 5.

Managing risks:
identifying, analyzing
and addressing risks



After the systematic description and legal analysis (including the assessment of the necessity and proportionality of the processing) have been carried out, it is time to implement the risk management.

Risk management is about:

- 1 identify the risks to the rights and freedoms of natural persons posed by the processing** (see section 5.1)
- 2 analyze the identified risks based on how likely they are to materialize and how serious it would be if they did** (see section 5.2)
- 3 describe the risk mitigation measures** (see section 5.3)
- 4 follow up on risks and reassess risks** (see section 5.4).

Often, the risks have already been assessed in a general way when the controller decided to carry out a DPIA. This initial risk assessment is often useful when the risks are assessed in the context of the impact assessment itself. The assessment and management of the risks can be carried out in one or more workshops involving people with different competences. If a Data Protection Officer has been appointed, he/she should be consulted in the context of the risk assessment and in the assessment of risk mitigation measures.



Template to support your work

Please use the Excel sheet Risk management in impact assessment to facilitate the execution of the risk management and the documentation of identified risks, risk analysis and identified risk mitigation measures.

All materials related to the practical guide can be found at imy.se/impactassessment



Remember!

There is a difference between risk and vulnerability assessments in the general information security work of the organization and the risk assessment to be carried out in the context of a data protection impact assessment. The latter aims to protect information when processing personal data and to ensure compliance with the GDPR. It is the protection of individuals' rights and freedoms that is relevant. Information security is instead generally about protecting all types of information that an organization handles. The purpose may be, for example, to maintain essential functions or the organization's own ability to operate.

5.1 Identifying the risks

In order to identify the risks that a particular personal data processing operation may pose to the rights and freedoms of individuals, you need to consider both internal and external factors. A prerequisite for identifying risks is that it is clear what types of personal data are to be processed, for what purposes and in what way.

It is crucial that risk assessment is done from the perspective of individuals. It is sometimes wrongly assumed that it is risks to the business that should be addressed at this stage. However, the risks to be identified, assessed and addressed in the context of a data protection impact assessment under Article 35 of the GDPR are only those relating to the rights and freedoms of individuals. Primarily their right to the protection of their personal data, privacy and integrity, but also other fundamental rights (e.g. freedom of expression, freedom of thought, freedom of movement, prohibition of discrimination, freedom of conscience and religion).

The concept of *risk* in the context of a DPIA can be defined as a shortcoming, weakness or vulnerability in the processing of personal data. It can also be a threat or an event related to a processing operation that could have a detrimental impact on compliance with data protection principles and adversely affect the rights and freedoms of individuals. These are therefore hypothetical scenarios with different consequences. Risks can stem from external threats (e.g. cyber-attacks or malware) or internal threats (e.g. misuse of data or lack of security measures in systems). Risks can arise from both intentional and unintentional actions.

In addition to risks of harm, controllers may need to consider risks of other types of adverse effects on individuals. Both for individuals affected by the processing in question (e.g. being subjected to discrimination, identity theft, financial loss or damage to reputation)³² and to society at large (e.g. loss of social trust).³³ Recital 75 of the GDPR gives more examples of what can be seen as risks to the rights and freedoms of natural persons.

Examples of risks and what they can lead to

- **Risk:** Too much information is stored via free text fields.
May lead to: Personal data being processed even though it is not necessary.
- **Risk:** Data is not deleted or segregated in time.
May lead to: Personal data being used for purposes other than the original ones.
- **Risk:** Authorization management is not applied in practice.
May lead to: Unauthorized access to the personal data.
- **Risk:** Sensitive personal data is not protected at a sufficient level of security in the production and testing environment.
May lead to: Unauthorized access to the personal data.

³² Recital 75 of the GDPR.

³³ Cf. Article 29 Working Party Opinion on a risk-based approach in the data protection legal framework (WP 218), p. 11.

- **Risk:** Procedures for logging and log follow-up are not followed.
May lead to: Unable to investigate incidents where unauthorized persons have accessed personal data, etc.
- **Risk:** Data is transferred to third countries without legal basis.
May lead to: There is no adequate level of protection for the personal data.
- **Risk:** There are deficiencies in purpose control.
May lead to: Personal data being used for purposes other than those originally intended.
- **Risk:** There are shortcomings in procedures to check the accuracy of personal data.
May lead to: Personal data is not accurate.
- **Risk:** Data subjects are insufficiently informed about the processing of their personal data.
May lead to: Individuals cannot exercise their rights under the GDPR.
- **Risk:** There are limited possibilities to contact representatives of the controller.
May lead to: Individuals cannot exercise their rights under the GDPR.
- **Risk:** There are shortcomings in data processor management procedures or insufficient control of compliance with these procedures.
May lead to: Personal data being disclosed to external parties who cannot guarantee sufficiently secure handling.



In-depth information

Annex Legal Interpretative Support: Section 4.1. Interpret Article 35(1) of the GDPR.

All materials related to the practical guide can be found at imy.se/impactassessment

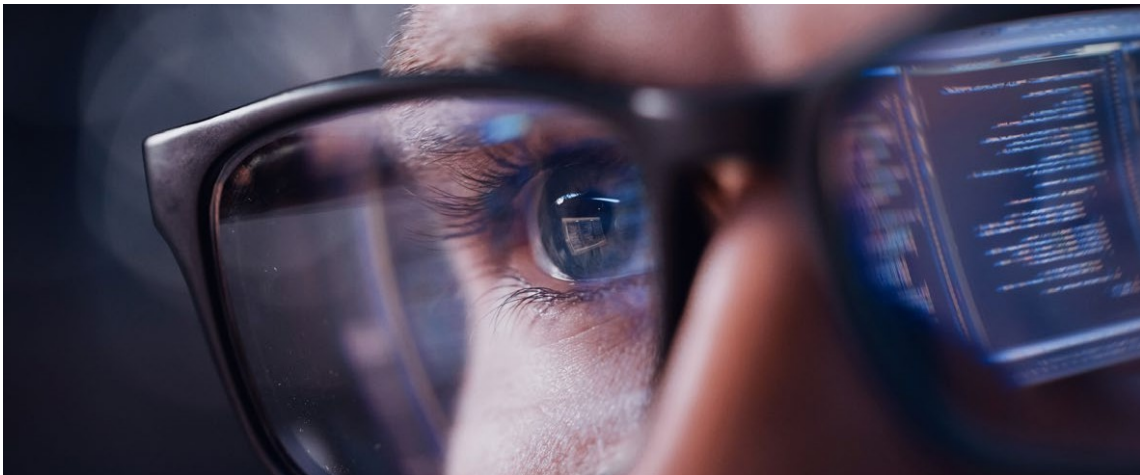
5.2 Analyze the risks

The purpose of the risk analysis is to assess the likelihood of an undesired event occurring and the severity of the event, based on an objective assessment of the nature, scope, context and purposes of the processing.³⁴ The objective nature of the assessment means that the risk to the rights and freedoms of individuals cannot be downplayed on the grounds that the business is trying to achieve its financial objectives, for example. The analysis of the likelihood and severity of the risks must be carried out so that the controller can then determine the appropriate measure(s) to mitigate the risks.

Assessing the likelihood of risks

In order to assess the likelihood of an identified risk materializing, the following aspects should be considered, among others.

- ***The type and scope of personal data***
The categories of personal data processed and the amount of data can affect the desirability of the data and increase the risks of adversarial threats.
- ***Experience and incident history***
By analyzing shortcomings and incidents in previous processing operations, the controller can identify patterns and trends that may affect the likelihood of an identified risk becoming a reality. It is important to take into account both incidents within the organization and the relevant industry.
- ***Effectiveness of security measures and controls***
By testing and evaluating the effectiveness and robustness of different security measures, and conducting internal checks before starting a personal data processing operation, the ability to prevent and minimize risks can be assessed. This can be done by evaluating technical security solutions and processes for handling personal data, as well as staff training.
- ***Continuous review***
Continuous review of processing and security measures can reduce the likelihood of risks occurring. The review of the likelihood should take place in connection with new or changed circumstances, such as a change of data processor, new technical features of a digital service or the entry into of new laws.



³⁴ Recitals 76 and 90 of the GDPR.

Assess the severity of the risks

In order to assess the potential severity of the unwanted event if it occurs, the following aspects should be considered, among others.

- **Impact on individual rights and freedoms**
A key factor to consider is how the unwanted event could harm the privacy of individuals or affect the ability of data subjects to exercise their rights under the GDPR.
- **Nature of the processing and type of personal data**
The severity of the risk in question is influenced by the type of processing involved and the personal data being processed. For example, if a risk involves data relating to children or sensitive personal data, the severity increases.
- **Scope of the risk**
The controller's assessment should include an analysis of how many individuals could potentially be affected if an identified risk actually occurs. The more people that could be affected, the more serious the risk.
- **The context of treatment**
In making this assessment, the controller should also consider whether the processing may be perceived as unpredictable. Aspects such as the controller's relationship with individuals and the extent to which individuals have control over their personal data should also be considered.

Carry out risk assessment

The next step in risk management is *risk assessment*, where the combination of assessed likelihood and severity is evaluated. The risk assessment can be carried out in different ways, depending on the type of personal data processing involved.

Risk, probability and severity can be described in running text or using a so-called risk matrix, where probability and severity are expressed as a number between e.g. 1-4 (from low to high probability or severity). A risk matrix *can* be a good tool to visualize and create an overview of the identified risks and the need to prioritize actions within an action plan. Based on the risk matrix and a combined numerical value of likelihood and severity, the controller can arrive at an overall assessment of the risk.

IMY's proposed approach and the impact assessment template developed by IMY do not use a risk matrix with a combined numerical value. Instead, likelihood and severity are categorized on a four-point scale, after which the overall risk assessment is described in running text. The reason is that it is difficult to convert assessments of the likelihood and severity of risks to individuals' rights and freedoms into a combined numerical value, and that the reasoning behind the assessments risks being lost.

5.3 Addressing the risks

Once the risk assessment has been carried out, it remains to identify appropriate technical and organizational security measures that can mitigate the risks and ensure a level of security appropriate to the risks. The measures should be tailored to address the specific risks of the processing in question, and be proportionate to the specific risk and the potential impact on the rights and freedoms of individuals. You should consider which measures are most effective and appropriate to address the identified risks.

Examples of risk mitigation measures to manage certain risks

The risk of collecting more personal data than necessary for the purposes of the processing due to the use of free text fields to collect data.

- Provide information related to free text fields on what data is required.
- Establish and implement regular checks, such as spot checks, that the data collected is necessary.

the risk that systems that are supposed to automatically delete data based on retention periods set do not work as intended; and that data are thus stored for longer than necessary.

- Conduct robust testing of the system.
- Introduce and carry out regular checks, such as spot checks on the performance of the system.

The risk that procedures for manual deletion of data based on the defined retention periods are not followed by staff, and that data are stored for longer than necessary.

- Conduct regular training and other activities to remind people of the importance of following manual deletion procedures.
- Ensure that procedures for manual thinning are easy to follow.
- Incorporate references to manual thinning procedures in relevant processes.
- Establish and carry out regular checks, such as spot checks on staff compliance with procedures. If deviations are detected, investigate the causes and take appropriate action.



The GDPR does not provide a practical approach to risk management. Therefore, there is an opportunity to integrate the risk management required by the GDPR with the organization's other risk management efforts and practices. It is important that the controller identifies who is responsible for carrying out risk mitigation tasks, both internally and in collaboration with other parties. This is to be able to continuously evaluate the effectiveness of the measures and to be able to report and correct any identified shortcomings or deal with incidents that occur. The need for controllers to be able to demonstrate compliance with the GDPR³⁵ means that the decision-making process, implementation and management of risk mitigation measures must be adequately documented.

Taking legal safeguards to exempt the organization from liability is not an acceptable management of the identified risks (for example, taking out an insurance policy to cover the damages that may be incurred by the organization, or entering into an agreement aimed at transferring liability to a third party, does not reduce the potential risks to individuals' rights and freedoms).

Depending on how the measures are designed and implemented, they may meet the requirements of several of Articles 5, 24, 25 and 32 of the GDPR. Different perspectives may result in different assessments of the level of security required to ensure adequate protection, although the measures taken to mitigate risks are often the same. For example, a firewall that filters out unwanted online traffic can protect against threats to both business capabilities and individual rights and freedoms. Encryption of information can protect both business-critical data and personal data from unauthorized access or disclosure.

³⁵ See Article 5(2) of the GDPR.

□ — **Examples of risk reduction measures**

□ — ***Technical measures***

- functions for authentication
- logging
- technical access restriction and access control
- encryption of information
- user-friendly and functional menus, flows and reporting features
- automatic checking of data that can alert the user in case of wrong input
- support for backup and recovery
- limiting search options (e.g. not being able to search on sensitive personal data)
- automatic deletion of personal data that is no longer to be processed
- anonymization of personal data
- pseudonymization of personal data
- privacy-enhancing technologies (PETs)
- technology to detect, manage and report incidents

Organizational measures

- decisions not to collect or store certain types of information
- tailored templates to ensure data minimization
- procedures for sorting and storage
- procedures for the granting of access rights
- clearly defined division of tasks for units and employees when processing personal data
- continuous information and training to employees on the decisions, procedures, restrictions, etc. that apply to personal data processing
- qualification requirements for staff authorized to process personal data
- confidentiality agreements for own or other staff with access to the personal data (e.g. IT staff)
- checks to ensure compliance with procedures and measures
- updated data processing agreements that clearly regulate access to and processing of personal data by data processors
- information and training for staff on how data subjects exercise their rights
- clear information to data subjects about the processing of personal data



Risk management in different sectors

Codes of conduct and certification can be useful to provide concrete guidance on how to identify risks and take risk mitigation measures. These are tailoring tailored to the specificities of a particular processing operation and adapted to the application of specific provisions to protect personal data under the GDPR.

In some cases, Union or national legislation may provide for specific protection measures to be taken by controllers when carrying out certain processing operations for specific purposes. An example of this from the healthcare sector is Chapter 4 of the Patient Data Act (2008:355) and the National Board of Health and Welfare's regulations and general guidelines on record keeping and processing of personal data in healthcare (HSLF-FS 2016:40).

5.4 Follow up and reassess risks

Once the mitigation measures have been identified, the risk assessment should be updated. The likelihood and severity shall be re-analyzed and a new risk assessment shall be performed. The new risk assessment, taking into account the risk mitigation measures, shall be reflected in the risk management documentation.

If risk mitigation measures are not feasible, or if the measures cannot sufficiently reduce the risk to the rights and freedoms of individuals, the controller needs to implement additional measures. If this is not possible, the options are not to carry out the planned processing or to request prior consultation with IMY.

Step 6.

Request prior consultation with IMY if risk remains high





If the risks remain high - despite the consideration of risk mitigation measures - the controller has an obligation to request prior consultation with the IMY before starting the processing.³⁶ This applies even if only one of the identified risks is deemed to remain high.

Article 36(3) of the GDPR specifies the documentation to be provided by the controller to the supervisory authority in the context of the request for prior consultation. In the case of a request for prior consultation, the impact assessment must be included as part of the documentation.³⁷ If an impact assessment is missing or deemed inadequate, IMY may request completion or reject the request for prior consultation.³⁸



Read more

IMY website imy.se - [Pre-consultation](#)

³⁶ Article 36 of the Data Protection Regulation.

³⁷ Article 36(3)(e) of the GDPR.

³⁸ Cf. Article 35(7) of the GDPR, which specifies the minimum content of an impact assessment.

Step 7.

Gather input from stakeholders



7.1 Recommendations from the Data Protection Officer

The GDPR requires that the DPO (if one has been appointed in the organization) be consulted in the impact assessment process³⁹.

The controller has some discretion to determine the manner and when the DPO should be involved. However, the DPO should be consulted on an ongoing basis, as early as possible and in relation to important decisions in the context of the impact assessment. In particular, the DPO should be consulted prior to the decision to carry out or not to carry out an impact assessment, and in the context of risk management. The DPO should also be given the opportunity to evaluate the outcome of the impact assessment.

The recommendations and opinions of the DPO at different stages of the impact assessment should generally be documented. The DPO should also prepare a separate written statement of the impact assessment, including how the DPO has been involved in its implementation and the documentation on which the statement is based. If the controller decides not to comply with a formal recommendation from the DPO, the controller should also document a justification for it.



In-depth information

Annex Legal Interpretative Support: Section 6. The role of the DPO in the impact assessment

All materials related to the practical guide can be found at imy.se/impactassessment

7.2 Comments from data subjects

When views need to be collected

The GDPR states that the controller must seek the views of data subjects "where".⁴⁰ This means that seeking such views is not optional, but where it must be done. Circumstances that indicate that it is appropriate are, for example, that the envisaged processing affects a large number of data subjects, involves sensitive personal data or involves automated decision-making.

One of the purposes of seeking the views of data subjects is to inform the risk assessment and other parts of the impact assessment. Therefore, the views should be sought at a time that allows the controller to take them into account. Data subjects should not be consulted after the risk assessment has been completed if the controller will not be able to reassess the risks based on the comments received. Sometimes it is appropriate to consult data subjects already before or during the risk assessment. Feedback can also help to clarify the appropriateness and proportionality of the processing to data subjects and give them more insight into how the business will process their personal data.

³⁹ E.g. Article 35(2) and Article 38 of the GDPR.

⁴⁰ Article 35(9) of the GDPR.

The views of the data subjects or their representatives are not binding on the controller. Regardless of the views of the data subjects on the intended processing, the risk assessment must be carried out in accordance with the requirements of the GDPR. Therefore, the controller cannot conclude that a planned processing operation is risk-free simply because the data subjects consulted have not identified any risks associated with the planned processing operation.

The fact that data subjects have given their consent to a processing operation does not mean that their views have been sought on the matter in question.⁴¹ Therefore, a controller cannot refrain from seeking views solely on the basis that data subjects have (or will have) consented to the intended processing, if it is otherwise appropriate to seek such views.⁴²

When comments do not need to be collected

The GDPR states that the controller does not need to seek the views of data subjects if this would affect the protection of commercial or public interests or the security of the processing. Examples of acceptable reasons for not seeking the views of data subjects are that it would jeopardize the company's business plans or other confidential information such as intellectual property or trade secrets. Other acceptable reasons may be that it is impracticable or that the effort is disproportionate to the risks likely to be posed by the processing or to the data subjects' ability to provide relevant comments on the processing⁽⁴³⁾.

Who should be consulted

Who to consult depends on the groups of people who will be affected by the risks of the processing. In particular, the controller should seek the views of data subjects who are likely to have important information or can provide views that are particularly relevant to the impact assessment.

The GDPR states that the views should be obtained from the *data subjects or their representatives*.⁴⁴ The concept should be interpreted broadly. It may concern, for example



41 Compare the concept of consent in Article 6(1)(a) of the GDPR with the rule on obtaining views in Article 35(9).

42 WP 248, p. 16 f.

43 See WP 248, p. 16 et seq.

44 Article 35(9) of the GDPR.

representatives of various organizations defending the interests of data subjects, or consumers in general.⁴⁵ For processing operations involving pupils in a school, it could be the pupils' guardians. For processing operations involving employees, the safety representative or the workers' organizations represented in the workplace may be consulted. Representatives may also, in some cases, be staff who work closely with the data subjects or who for other reasons have a good insight into their interests.

If a proposed processing operation only poses risks to a limited number of data subjects, it may be sufficient to seek the views of representatives of particular group. For example, for processing operations concerning employees, it may be appropriate to consult a number of employees or their trade union representatives. On the other hand, if the proposed processing operation poses risks to a large number of natural persons who have not yet been identified (e.g. all residents), it may be appropriate to find out how potential data subjects generally perceive a particular processing operation⁴⁶.

How data subjects' views should be collected

The way in which the views are collected depends, among other things, on who is to be consulted, the type of information required for the data subjects to understand the meaning of the intended processing and what is a proportionate effort in relation the risks of the processing. For example, the collection may take the form of a questionnaire. If a controller already has contacts in the form of, for example, reference groups, user groups or opinion panels, it may be appropriate to use these.

Questions should be clearly defined and formulated in a way that is easy to understand. To avoid "information fatigue", the survey should be as concise as possible.⁴⁷ Respondents should be given sufficient time to answer the questions. In order to allow data subjects to actually take a position on the intended processing, the controller itself should describe the risk factors identified by the business.

Document the comments

As a rule, it is sufficient to document the views of the data subjects by compiling the results of the survey. If the controller decides to proceed with the processing despite the data subject's views to the contrary, a justification should be documented. A controller that decides not to obtain the data subject's views should also document a justification for that.⁴⁸

7.3 Comments from other stakeholders

In some cases, there may be stakeholders other than data subjects whose views should be sought and documented in the impact assessment (for example, from information security officers or other people in the organization with technical expertise).

⁴⁵ See WP 248, p. 16 et seq.

⁴⁶ See WP 248, p. 16 et seq.

⁴⁷ For guidance on transparency and information to data subjects, see e.g. Article 29 Working Party Guidelines on Transparency under Regulation (EU) 2016/679 (WP 260 rev. 01). The EDPB has endorsed the guidelines, Endorsement 1/2018.

⁴⁸ See WP 248, p. 17.

Step 8.

Make an overall assessment



By the time you get to this stage, the risks of the envisaged personal data processing have been managed and the obligation to request prior consultation assessed.

Information may have become available which is relevant and should be taken into account, and which makes it appropriate to make an overall assessment of whether the processing can be carried out. In this step, the controller should consider whether the identified risks can still be considered to be adequately managed, and whether the envisaged processing can still be considered necessary and proportionate in relation to its purpose.



Step 9.

Embedding the assessment in the organization



Authorized persons in the management of the controller organization shall be informed of the impact assessment, the identified risks, the risk assessment and the identified risk mitigation measures.

Each organization should have an established process for how to do this. The GDPR does not contain any rules on how the impact assessment should be embedded within the controller organization. This can be done, for example, by providing management with a summary of the final results of the impact assessment and the necessary justifications. It should be made clear who or which function in the organization is responsible for implementing the risk mitigation measures. Responsibility for any residual risk of the treatment should also be clarified.



Step 10.

Follow up the impact assessment continuously



A DPIA is not a one-off event but a process. This means controllers need to check, where necessary, whether the processing is carried out in accordance with the impact assessment and review if risks change.⁴⁹

It is often appropriate to build the review of impact assessments into the other processes and systematic work of the business, for example in annual cycles or other regular reviews. The appropriate time interval for reviewing existing impact assessments depends, among other things, on the risks of the treatment and technology used. The first review should always be carried out relatively close to the start of treatment, preferably after about one year. Thereafter, the impact assessment should be as a starting point, be reviewed every two years. The review should be more frequent in the case of use of new technologies, large-scale processing or processing involving sensitive personal data. For processing operations that are well-tested or well-established however, the review may take place less frequently than every two years.

The requirement for regular review is in addition to the review that must be done if the risk picture changes. If the risk changes, the controller must assess whether the processing is still carried out in accordance with the original impact assessment or whether it needs to be updated. The risk picture may change due to factors that are due to their own activities (e.g. organizational changes), or due to factors external to their own activities (e.g. a change in the legal or external environment), or a combination of both.

It is important that the controller ensures that any changes in risk are captured within the organization, for example through procedures and clear accountability.

□ — Examples of when risks can change

- — • new technology is introduced in the treatment (e.g. an AI model)
- — • more data than expected is collected (e.g. if a system that previously only processed name and address information is proposed to process data of a more sensitive nature)
- — • there are important changes at societal level (e.g. some automated decisions have a greater practical impact on individuals than before, or new categories of data subjects become vulnerable to discrimination)
- — • the controller discovers a security breach that shows that the risk was higher than previously thought (e.g. through a data breach).

⁴⁹ See Article 35(11) of the GDPR.

Sources

In addition to the GDPR, the guidance is mainly based on

- Judgments of the Court of Justice of the European Union (see footnotes).
- [IMY's list pursuant to Article 35\(4\) of the Data Protection Regulation dated January 16, 2019 and related decision \(No. DI-2018-13200\) \(IMY's list pursuant to Article 35\(4\) of the Data Protection Regulation\)](#).
- [Guidelines of the European Data Protection Board \(EDPB\) and its predecessor the Article 29 Working Party:](#)
 - *Statement on the role of a risk-based approach in data protection legal frameworks* (WP 218), adopted on 30 May 2014.
 - *Guidelines on Data Protection Officers* (WP 243 rev. 01), last reviewed and adopted on April 5, 2017.
 - *Guidelines on data protection impact assessment and determining whether processing is "likely to result in a high risk" within the meaning of Regulation 2016/679* (WP 248 rev. 01), adopted on April 4, 2017 and revised on October 4, 2017.
 - *Guidelines on automated individual decision-making and profiling under Regulation (EU) 2016/679* (WP 251 rev 01), last reviewed and adopted on 6 February 2018.
 - *Guidelines on transparency under Regulation (EU) 2016/679* (WP 260 rev. 01), last reviewed and adopted on April 11, 2018.
 - *Guidelines 3/2019 on the processing of personal data by video devices*, version 2.0, adopted on January 29, 2020.
 - *Guidelines 07/2020 on the concepts of controller processor in the GDPR*, version 2.1, adopted on July 7, 2021.
- IMY supervisory decisions related to Article 35 of the GDPR.
- Information provided by other European Data Protection Authorities on their websites on impact assessments.
- Doctrine (shown in footnotes).

This is the Data Protection Authority

The Data Protection Authority works to protect all your personal data, such as health and financial information, so that it is handled correctly and does not fall into the wrong hands. We are the ones who check that companies, public authorities and other actors comply with the GDPR - the General Data Protection Regulation.

the General Data Protection Regulation. We train and guide those who process personal data. We want to see a sustainable and privacy-friendly digitalization. We are convinced that it is possible to ensure the safety of citizens and the security of society without unjustified mapping and surveillance. Together with the other data protection authorities in the EU, we are working to ensure that citizens' personal data protected equally across the Union. We are also working to ensure credit checks are carried out correctly.

Our vision is a secure information society, where we work together to protect privacy.

Contact the Data Protection Authority

E-mail: imy@imy.se

Web: www.imy.se

Tel: 08-657 61 00

Postal address: Integritetsskyddsmyndigheten,
Box 8114, 104 20 Stockholm