IMY Integritetsskydds myndigheten

IMY's template for

Assessment of the need for an impact assessment under the GDPR

Equivalent to Step 1 of *A Practical Guide*

About the template

The template corresponds to Step 1 of the Practical Guide. The template is intended to help you, as a data controller, to document in a structured way the assessment of the need to carry out a data protection impact assessment in accordance with Article 35 of the GDPR[1].

When assessing whether an impact assessment is mandatory, the person responsible for the data must be taken into account:

- the factors listed in Article 35(1) of the GDPR
- the examples in Article 35(3) of the GDPR
- IMY's list under Article 35(4) of the GDPR (based the criteria set out in the EDPB Guidelines on Impact Assessment).

Read more about the assessment of the need for an impact assessment

A practical guide: Step 1
Annex Legal interpretative support: section 4
All materials can be found at imy.se/impactassessment

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

Documentation

In the template, the space for notes is limited. If you need more space for your documentation, you can refer to an annex.

Remember!

It *is the type of treatment* that is relevant assessing the need for an impact assessment. Therefore, measures to reduce or eliminate risks of the individual planned treatment cannot be considered in this assessment.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons 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).

General information

Roller

Identify the controller of the envisaged processing operation and the roles involved in assessing the need to carry out an impact assessment.

Data controller	
Data processor(s)	
The roles involved in the assessment	
Person responsible for assessing the need to carry out an impact assessment	

Planned processing of personal data

Describe in general terms the treatment envisaged, for example the service, process or system to be implemented.

Step 1. Assess the need to carry out an impact assessment

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

Use the factors set out in Article 35(1) of the GDPR to determine whether it is a type of processing likely to result in a high risk to the rights and freedoms of natural persons, which requires an impact assessment.

- Use of new technologies
- Nature of the treatment
- Scope of the treatment
- The context of treatment
- Purpose of the treatment

For more information on the meaning of the factors, see the annex Legal interpretative support - section 4.1.

Question: Taking these factors into account, is there already a case for carrying out an impact assessment?

The examples in Article 35(3) of the GDPR

a. A systematic and comprehensive assessment of personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions having legal effects on natural persons or similarly significantly affecting natural persons are based.
b. 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.
c. Systematic monitoring of a public place on a large scale.

For more information on the interpretation of Article 35(3)(a) to (c) of the GDPR, see the Legal Interpretative Support Annex - section 4.2.

Question: Does the envisaged processing correspond or resemble any of the examples in Article 35(3) of the GDPR (see above)?

☐ Yes

☐ No

IMY's list under Article 35(4) of the GDPR

The main rule is that if a planned treatment meets at least two of the criteria in IMY's list under Article 35(4) of the GDPR, a consistency assessment must be carried out. 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.

If the controller assesses that the type of processing in an individual case is unlikely to result in a high risk, even though two or more of the criteria are met, a detailed justification for this must be documented.

Question: Which of the criteria in the list are met?		
Criterion	**Example**	**Answer.**
1. does the treatment involve the evaluation or scoring of people?	A company offering genetic tests to consumers to assess and predict disease risks, a credit reference agency or a company profiling internet users.	☐ Yes ☐ No
2. is personal data processed for purpose of taking automated decisions which legal effects or similarly significant effects on the data subject?		☐ Yes ☐ No
3. does the treatment involve systematic monitoring of people?	Through camera surveillance of a public place or by collecting personal data from internet use in public environments	☐ Yes ☐ No
4. Are sensitive personal data under Article 9 or data of a highly personal nature processed?	A hospital storing patient records, a company collecting location data or a bank handling financial data	☐ Yes ☐ No
5. Is personal data processed on a large scale?		☐ Yes ☐ No
6. Is personal data from two or more processing operations combined in a way that deviates from what the data subjects could reasonably expect?	Interconnection of registers	☐ Yes ☐ No
7. Are personal data of persons who for any reason are in a disadvantaged or dependent position and therefore vulnerable processed?	Children, workers, asylum seekers, elderly and patients	☐ Yes ☐ No
8. are new technologies or organizational solutions used?	Internet of things (IoT) application	☐ Yes ☐ No

Question: Which of the criteria in the list are met?		
Criterion	**Example**	**Answer.**
9. is personal data processed for the purpose of preventing data subjects from a service or entering into a contract?	When a bank checks its customers against a credit reference database to decide whether to offer them a loan.	☐ Yes ☐ No

For more information on IMY's list under Article 35(4) of the GDPR, see the Legal Interpretative Support Annex - section 4.3.

Question: Are two or more of the criteria in the list met?

☐ Yes (the general rule that an impact assessment must be carried out is therefore fulfilled) No

☐

Question: If the answer is yes, is the assessment that *the type of treatment* does not require an impact assessment to be carried out anyway?

☐ Yes (please provide a detailed justification for your

☐ answer below) No

Question: If no, is the assessment that *the type of treatment* means that an impact assessment should be carried out anyway?

☐ Yes (please give reasons

☐ below) No

No obligation to carry out an impact assessment

Question: Is the treatment very similar to a treatment for which an impact assessment has already been carried out?

☐ Yes (please elaborate

☐ below) No

Question: Is the processing subject to a general impact assessment under Article 35.10 of the GDPR?

☐ Yes (please elaborate

☐ below) No

Consult the Data Protection Officer

If two or more of the criteria are met and the controller nevertheless considers not carrying out a DPIA, the DPO (if appointed) should be consulted. The DPO can provide his/her assessment below and then return the document to the controller.

Question: Does the DPO agree that an impact assessment should not be carried out? (Where at least two criteria in the list are met, the answer should be developed in detail).

☐ Yes (give reasons below) No

☐ (give reasons below) Not

☐ applicable

Question: Does the Data Protection Officer have any recommendations?

☐ Yes (indicate these in the table

☐ below) No

No	Recommendation of the Data Protection Officer	date	Controller's response to the recommendation
001			☐ Accepts ☐ Accept and take action Reject If the DPO's recommendations are rejected, provide a detailed justification below.
002			☐ Accepts ☐ Accept and take action Reject If the DPO's recommendations are rejected, provide a detailed justification below.
003			☐ Accepts ☐ Accept and take action Reject If the DPO's recommendations are rejected, provide a detailed justification below.

Conclusion

Question: Does the controller consider that there is a need to carry out an impact assessment prior to the intended processing?

☐ Yes

☐ No