IMY Integritetsskydds myndigheten

IMY's template for

Data protection impact assessment under the GDPR

Corresponds to Steps 3-10 in *A Practical Guide*

Contents

About the template

The template corresponds to steps 3-10 of the Practical Guide. The guide provides more information on each step. The Excel sheet Risk management in impact assessment can be used in Step 5.

The practical guide and templates can be found at imy.se/impactassessment The

template is intended to make it easier for data controllers to document a data protection impact assessment under Article 35 in the General Data Protection Regulation[1].

Please note that some of the steps may need to be carried out in a different order. For example, in some cases it may be appropriate to seek input from data subjects at an earlier stage. If the controller has appointed a data protection officer, this should be consulted on an ongoing basis.

Documentation

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

[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

Controller of the processing	
Organization (including organization number)	
Address	
Phone number	
E-mail address	

Contact details of the Data Protection Officer	
Organization's Data Protection Officer	
Address	
Phone number	
E-mail address	

Persons responsible for the impact assessment	
Person responsible for carrying out the impact assessment	
Responsible for the content of the impact assessment and the assessments which are made	
Roles involved in carrying out the impact assessment	
Responsible for managing any residual risks after the impact assessment has been completed	
Responsible for following up the impact assessment	

Step 3. Systematic description of the personal data processing

3.1 Nature of the treatment

General description and background

Instructions

Define and describe the object of the impact assessment. Provide a background and describe the reasons for the planned treatment.

Categories of personal data

Instructions

List the categories of personal data that will be processed. Use one row for each category and add as many rows to the table as necessary. If the table is extensive, it may be appropriate to put it as an annex to the impact assessment instead.

Indicate in the right column if any of the following categories apply:

- categories of personal data listed in Articles 9 and 10 of the GDPR
- personal data that is sensitive to privacy for other reasons (e.g. because it relates to individuals' financial or personal circumstances)
- social security number or coordination number

Category of personal data	Special category of personal data

Categories of registrants

Instructions

List the categories of data subjects whose personal data will be processed. Use one row for each category and add as many rows to the table as necessary. If the table is extensive, it may be appropriate to annex it to the impact assessment instead.

Indicate in the right column if any of the following categories apply:

- dependent persons (e.g. employees, patients or students)
- children or other vulnerable people (e.g. elderly, or people with disabilities)

Category of registrants	Special category of registrants

3.2 Scope of the treatment

Volume of the treatment

Instructions

Estimate the number of individuals concerned by the processing and the total amount of personal data that will be processed. Also describe the number of categories of personal data (the variety).

Take into account how often personal data will be .

Geographical scope of treatment

Instructions

Describe in which countries the data will be processed. Indicate if the countries involved will be outside the EU/EEA, so-called third country transfers.

3.3 The context of treatment

Instructions

Describe the treatment in a broader perspective, i.e. the internal and external factors relevant to the context in which the treatment will take place.

3.4 Purpose of the treatment

Instructions

Describe the reason why the controller wants to carry out the processing and the benefits of the processing (e.g. for the business, the public and third parties). Also describe the intended outcome for individuals. The purpose should be as precise, detailed and clear as possible.

3.5 Necessary resources

Instructions

Describe the resources and information assets needed to carry out the personal data processing (e.g. software, servers, hardware, networks, cloud services, etc.)

3.6 Functional description of the treatment

Instructions

Describe in more detail how the processing will take place and where the personal data come from. If the processing is complex, it may be appropriate to refer to an annex containing a flowchart, table or similar.

3.7 Roles and responsibilities

Personal data liability

Instructions

Specify the controller(s), i.e. the actors who alone or jointly determine the purposes and means of the processing of personal data. Indicate whether the processing involves separate or joint responsibility of the controllers.

List the contractual documents that specify the division of responsibilities between the data controllers.

Recipients including data processors

Instructions

Indicate whether personal data will be transferred to external recipients and if so, which ones. Please also indicate whether personal data processors will be involved in the processing and what services they will provide.

List any data processing agreements.

Data processor	Categories of personal data processed by the processor	Purposes of the processing by the Assistant

Step 4. Legal analysis

4.1 Existing regulations

Instructions

Make an inventory of the regulatory framework applicable to the processing in question. Also take into account adopted codes of conduct, implemented certifications and industry practices.

4.2 Data protection principles and the legal basis for processing

The principle of legality, regularity and transparency

Instructions

Describe how you ensure compliance with the principle.

Legal basis for processing

Instructions

Specify the legal basis for processing personal data. Be sure to indicate if there are several legal bases, i.e. if different categories of personal data or different stages of processing are supported by different legal bases.

- If the legal basis is *consent*, the description should indicate how consent is documented and administered and how the data subject can withdraw consent.
- If the legal basis is *balancing of interests*, the assessment made in balancing the interests of the controller and the interests of the data subjects should be carefully documented.

Description of the treatment (if applicable)	Personal data processed	Legal basis	Commentary
Example: Personal data is , stored and read in the customer portal service for error reporting.	Example: Name E-mail address Customer number Correspondence with customer service staff	Example: Art 6.1 b - Contracts	Example: The service contract includes the handling of fault reports from customers.

Legal basis for processing certain categories of personal data

Instructions		
If special categories or particular applicable to the processing • For specific categories of persons • For personal data relating to sheep see Article 10 of the Data Protection Regulation • For social security numbers and samosas	b (in addition to the legal basis above). sonal data: see exceptions in Article sentences in criminal cases, and the review of the law number: see section 10 of the Data Protection	ehandled, specify which exception 9(2) of the General Data Protection Regulation. involving criminal offenses: agent[2]
Personal data	**Applicable exception**	**Commentary**
Example: Data on health	Example: Article 9(2)(h)	Example: The treatment is necessary for health professionals to be able to keep records of patients' visits.

[2] Act (2018:218) with supplementary provisions to the EU General Data Protection Regulation

The principle of purpose limitation

Instructions

Describe how you ensure compliance with the principle.

The principle of data minimization

Instructions	
Describe how you ensure compliance with the principle.	
Personal data	**The processing is necessary in order to**
Example: Email address Example: Social security number	Example: Communicating with the data subject Example: Ensuring the identity of the data subject

The principle of accuracy

Instructions
Describe how you ensure compliance with the principle.

The principle of storage minimization

Instructions
Describe how you ensure compliance with the principle.

The principle of privacy and confidentiality

Instructions
Describe how you ensure compliance with the principle.

4.3 Rights of data subjects

Instructions

Describe what procedures the organization has in place to ensure that the rights of data subjects under the GDPR are respected, i.e.

- The right to information
- Right of access
- Right of rectification
- Right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object
- The right not to be subject to a decision based solely on automated processing, including profiling

Where there are procedural documents that are deemed to provide a sufficiently detailed description, reference may be made to these.

4.4 Safeguards for international transfers

Instructions

If personal data will be transferred to a country outside the EU/EEA in the context of the processing, please indicate the safeguards put in place below.

4.5 Overall assessment

Instructions

Indicate the overall assessment of whether the legal conditions for carrying out the processing are met (including the assessment of the necessity and proportionality of the processing in relation to its purposes).

Step 5. Risk management

Instructions

Feel free to use the Risk Management in Impact Assessment Excel sheet to

1. identify risks
2. analyze the probability and severity of risks
   - The likelihood of the risk being realized can be indicated as low, medium, high and very high.
   - The severity of the impacts can be assessed as limited, relatively severe, severe and very severe.
3. describe the risk mitigation measures; and
4. follow up the risks through a new risk assessment.

Summarize the assessment below.

Step 6. Assessment of the obligation request prior consultation

Instructions

Document the assessment of whether the risks remain high after the mitigation measures have been taken into account.

The outcome of any prior consultation

Instructions

Document the outcome of any prior consultation or attach the IMY's opinion.

Step 7. Comments collected from stakeholders

7.1 Recommendations of the Data Protection Officer

Instructions

Document any comments and/or recommendations made by the DPO in the course of the work. Also document any final statements made by the DPO.

Document and justify any decision not to follow formal recommendations from the DPO.

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.

7.2 Comments from data subjects

Instructions

Please indicate below if you have collected feedback from data subjects. Please also indicate if feedback has not been collected and if so, why.

Document any comments made by data subjects. Also justify and document any decisions that go against the views of data subjects.

Please note that data subjects may need to be consulted already before or during the risk assessment. Controllers may need to reassess the risks according to the comments.

7.3 Comments from other stakeholders

Instructions

Indicate whether you have sought input from any other stakeholder, such as an information security officer or someone with specific technical expertise. Document any input from them, if appropriate.

Step 8. Overall assessment

Instructions

Please provide the overall assessment of whether the planned treatment is feasible or not.

Step 9. Embedding the assessment in the organization

Instructions

Document how and when the descriptions and assessments you have made have been anchored in the organization's management team, for example through an internal referral or presentation at a management team meeting or similar.

Clarify who is responsible for taking the risk reduction measures and who is responsible for any residual risk associated with the treatment.

Step 10. Continuous review

10.1 Plan to implement the review

Instructions

Indicate when and how often the impact assessment will be followed up and which roles or functions in the organization are responsible for the follow-up. Also describe how it will be ensured that any changes to the risk are captured within the organization.

10.2 Version history

Instructions

Fill in the table to clarify when changes to the impact assessment have been made.

Version	date	Participants	Established by	Amendments
1.0	202x-xx-xx			