\*\* FREE PREVIEW VERSION \*\*

[organization logo]

[organization name]

**DATA PROTECTION IMPACT ASSESSMENT METHODOLOGY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc496564390)

[2. Reference documents 3](#_Toc496564391)

[3. Definitions 3](#_Toc496564392)

[4. General responsibilities for the DPIA 4](#_Toc496564393)

[5. Steps in the DPIA 4](#_Toc496564394)

[5.1. Step 1: Listing and grouping data processing activities 4](#_Toc496564395)

[5.2. Step 2: Answering threshold questionnaire 4](#_Toc496564396)

[5.3. Step 3: Determine whether a full data protection impact assessment is needed 5](#_Toc496564397)

[5.4. Step 4: Answer the Data Protection Impact Assessment Questionnaire 5](#_Toc496564398)

[5.5. Step 5: Identify and list key security risks 5](#_Toc496564399)

[5.6. Step 6: Determine how to mitigate the risks 5](#_Toc496564400)

[5.7. Step 7: Record the implementation 5](#_Toc496564401)

[6. Consultations with the supervisory authority 5](#_Toc496564402)

[7. Regular review of the DPIA 6](#_Toc496564403)

[8. Managing records kept on the basis of this document 6](#_Toc496564404)

[9. Validity and document management 6](#_Toc496564405)

# Purpose, scope and users

This methodology supports the Data Protection Impact Assessment (DPIA) in all business departments of [Company Name] (further: the “Company”).

This methodology describes the DPIA method and steps, and provides the required assessment criteria and reference examples.

The users of this document are Data Protection Officer, and the responsible persons in data protection activities.

# Reference documents

* EU GDPR Article 35
* EU GDPR recitals 75, 84, 89, 90, 91, 92, 93
* Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679

# Definitions

The following definitions of terms used in this document are drawn from Article 4 of the European Union’s General Data Protection Regulation:

**Personal data**: Any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is a natural person who can be identified, directly or indirectly, by reference to such information as name, ID card number, location, and other identifiable information, or one or more factors specific to the person's physical, physiological, mental, economic, cultural, or social identity, and other relevant information. Personal data includes a natural person's email address, telephone number, biometric features (such as fingerprint), location, IP address, health information, religious belief, social security number, and marital status.

**Sensitive personal data**:Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <https://advisera.com/eugdpracademy/documentation/data-protection-impact-assessment-methodology/>