1. Purpose

[XYZ] is fully committed to protecting the privacy of all relevant interested parties, including employees, customers, and suppliers as per the requirements of the General Data Protection Regulation (GDPR). Considering the critical importance of personal data privacy, various controls that ensure appropriate personal data collection and protection have been incorporated.

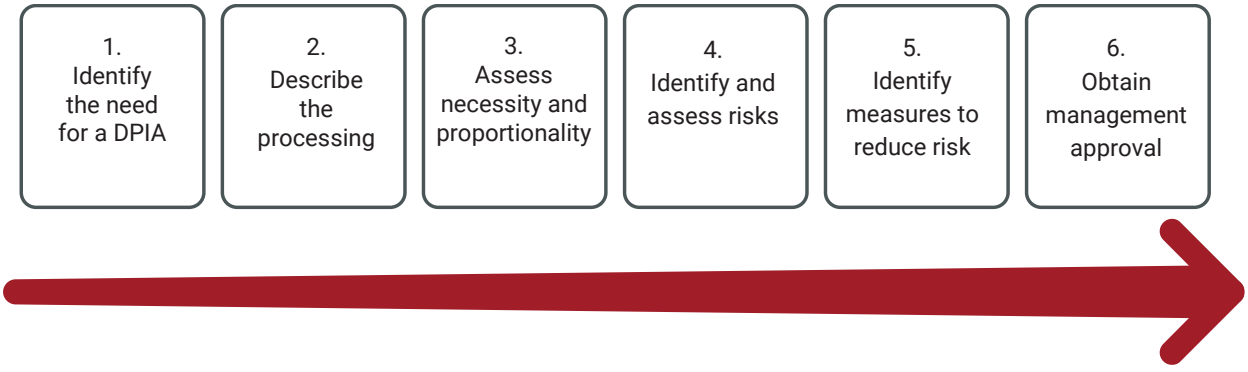
[XYZ] should ensure that any activity or project that includes the processing of personal data is subject to the data protection impact assessment (DPIA). The purpose of DPIA is to accurately identify, assess, and minimize the risks of data processing projects by putting in place the most appropriate mitigation measures which should ensure the rights and freedoms of individuals whose personal data are being processed.

This document describes the process of conducting a data protection impact assessment to ensure the fulfillment of objectives related to this subject matter.

1.1 Main Definitions from GDPR

Term	Definition
Personal data	*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*
Processing	*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*
Controller	*the 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*
Processor	*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*

2. Data Protection Impact Assessment Process



2.1 Identify the Need for a DPIA

There are various criteria to be considered by **[XYZ]** that determine when a data protection impact assessment should be carried out. According to GDPR (Article 35), a data protection impact assessment is required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) a systematic monitoring of a publicly accessible area on a large scale.

Note: Article 9(1) emphasizes that *the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, 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 shall be prohibited.*

Some certain conditions that require a DPIA include:

- Usage of new technologies
- Tracking of person’s location or behavior
- Collection and processing of personal data for the first time
- Sharing of personal data with persons or organizations that previously did not have access to them
- Usage of personal data processing to make automated decisions
- Processing of children’s data

Data processing activities are defined by taking into account the amount of data being processed, the number of data subjects, the categories from which the data should be collected, the frequency of data collection process and usage, and the geographical locations included. Any exclusion from the scope should be stated and justified.

In cases when there are uncertainties regarding the appropriateness of carrying out a DPIA, the Data Protection Officer should be consulted for clarification and further guidance.

2.2 Describe the Processing

A full description of the processing activities regarding personal data of individuals should be provided and documented. Such a description should include:

- The objectives of data processing

- The importance and necessity of data processing to achieve the organization's objectives
- The way data should be collected, processed, and stored
- The circumstances under which data may be transferred
- The persons that should have access to data
- The persons that will be affected by such processing, etc.

All this information can be collected by combining different relevant data mapping tools, including:

1. Data protection impact assessment questionnaire
2. Personal data analysis form
3. Personal data analysis diagram

2.3 Assess Necessity and Proportionality

The organization must have a lawful basis for engaging in data processing activities.

Each project or activity, regardless of the organization's size, type, or field of activity, must be stopped if there is no lawful basis or strong reason for engaging in such projects or activities.

In order to assess the necessity and proportionality of data-related projects or activities, the following should be addressed:

- The purpose of the data processing
- Other methods that can produce the same desired outcome
- Data minimization and data quality
- Information revealed to data subjects
- The way the rights of data subjects are to be supported during the processing
- The methods used for international transfers of the data

Some questions that might help in assessing necessity and proportionality are:

- What is the lawful basis for processing data?
- How do you guarantee the quality of the information?
- How do you plan minimization of information?
- How do you plan to provide people with privacy data?
- How do you implement and support individuals' rights?
- Do the taken measures guarantee compliance with your processors?

If the processing does not have a lawful basis or does not fit the purpose, issues will be evident regardless the identification of risks in the later stages of a DPIA.

2.4 Identify and Assess Risk

The "rights and freedoms of the data subject" refers to the privacy rights but including here also: the freedom of speech, of thought, and of movement. Depending on the

circumstances or the nature of the processing, other effects on the data subject may be considered as well.

A. Identify Risk Scenarios

Risks should be identified through interviews with all relevant interested parties, including:

- Managers of each project or activity
- Individuals responsible for carrying out project activities
- Data subjects
- Individuals providing supporting services and resources
- Recipients of the outputs of the project or activities
- Other parties' opinions considered useful for the risk identification process

All identified risks should be documented and risk owners should be assigned.

B. Analyze the Risk

The level of risk (high, medium, or low) should be assessed and calculated to determine both the likelihood and its potential impact on individuals.

C. Likelihood Assessment

An estimation of the risk likelihood should be made by taking into account the history of each identified risk — whether it has happened before within the **[XYZ]**, to other organizations in the same industry, or whether it has the capabilities to occur.

The likelihood of each risk should be graded on a numerical scale as presented below:

Rating	Probability of occurrence	Summary
1	Unlikely	Risk could happen but probably will not.
2	Possible	Risk is more likely to happen than not (between low and high).
3	Likely	There is a strong probability that risk can happen.

The rationale of the rate allocation should be documented and kept as evidence for future reference.

D. Impact Assessment

The impact of risk on the rights and freedoms of the data subjects should be assessed. However, the impact of risk should be greatly considered in areas such as:

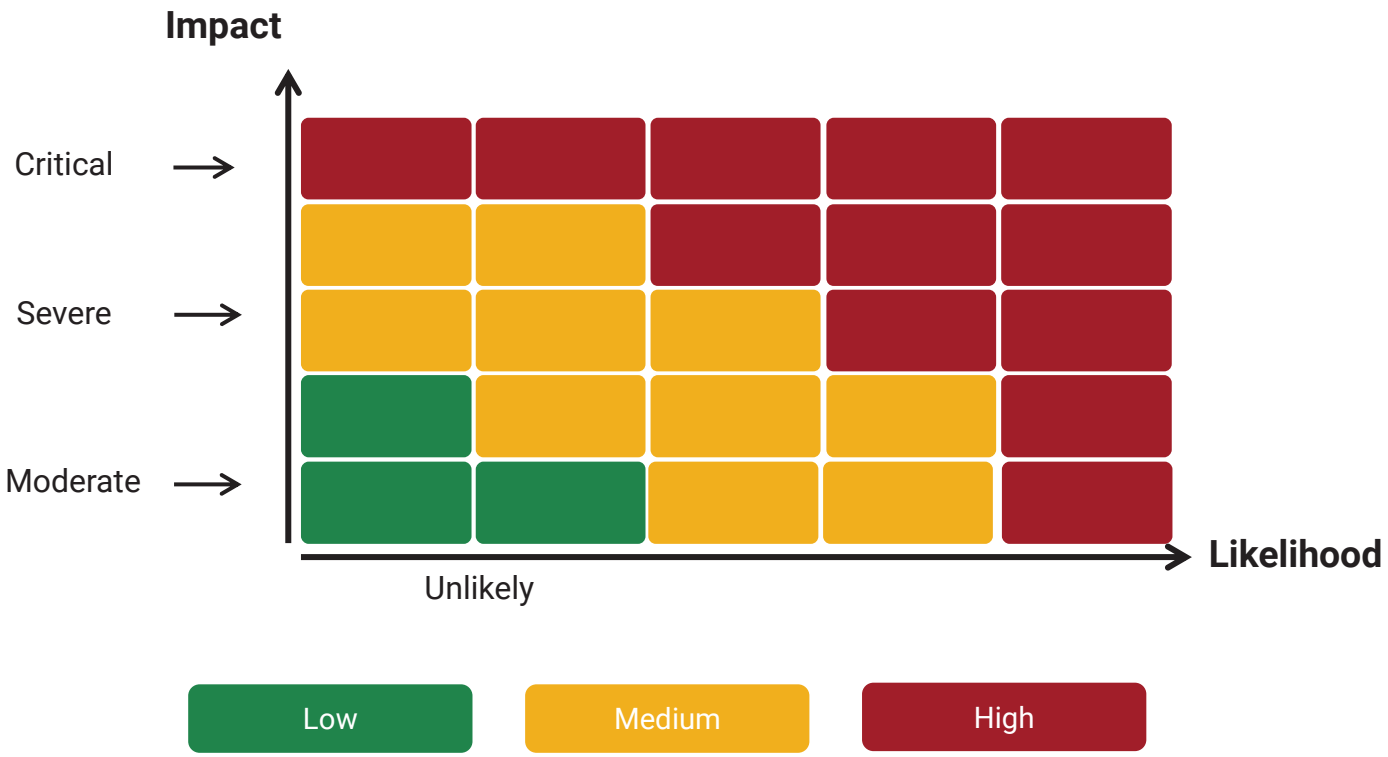
- Financial
- Health and safety
- Reputation
- Legal, contractual, or regulatory obligations

The impact of each risk should be graded on a numerical scale as presented below:

Rating	Description	Summary
1	Moderate	This presents a minor issue that does not lead to significant damage.
2	Severe	This will bring significant damage to a small number of data subjects or minor damage to a large number of data subjects.
3	Critical	This will bring significant damage to a large number of data subjects.

The rationale of the rate allocation should be documented and kept as evidence for future reference.

The assessment of risk likelihood and impact grading should be used to determine the level of risk based on the following risk matrix chart:



Note: Each risk should be allocated a classification score based on the general risk appetite of the project or activities.

The outputs of each risk classification should be used as input for the next stage of the DPIA — identifying measures to reduce risks.

2.5 Identify Measures to Reduce Risk

Once the risks are identified and classified, the organization should find ways on how to address each risk that is below the acceptable threshold. Risks should be treated according to the score and classification, i.e., very high scoring risks should be treated before those of lower levels.

A. Risk Treatment

Risks that have been considered by **[XYZ]** as unacceptable should be treated appropriately with one of the following options:

- **Risk reduction:** Additional controls should be applied if there is still some residual risk.

- **Risk avoidance:** Activities should be cancelled or modified if the identified risks are considered too high.
- **Risk retention:** Risk should be retained if it meets the risk criteria and there is no need to implement additional controls**.**
- **Risk transfer:** Certain risks should be shared with external parties, i.e., insurance or outsourcing.

When deciding which risk treatment plan to apply, **[XYZ]** should use rational judgement based on the circumstances surrounding the risk, such as:

- Business strategy
- Legal and regulatory agreements
- Technical issues

[XYZ] should ensure that all relevant interested parties are involved in defining the risk treatment plan.

B. Selection of Controls

Appropriate controls (i.e., actions to be taken to address risk) will then be known to either decrease the probability or effect (or both) of each risk to be within acceptable limits.

According to **[XYZ]**, the adoption of Annex A of ISO/IEC 27001 should be used as a point of departure for identifying suitable controls to address the risk treatment requirements identified as part of the risk assessment. The Annex A controls shall be complemented by the additional guidance presented in the following documents:

- *ISO/IEC 27002 — Information technology — Security techniques — Code of practice for information security controls*
- *ISO/IEC 27017 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 2702 for cloud services*
- *ISO/IEC 27018 — Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

C. Data Protection Impact Assessment Report

Once the treatment plan is implemented, **[XYZ]** should have a detailed data protection impact assessment report which should include:

- Processing activities and the amount of personal data involved
- Purposes of the processing
- Necessity and proportionality of the processing
- Assessment of the risk impact to the rights and freedoms of the data subjects
- Priority of risks for treatment
- Risk treatment option and controls to be implemented (if applicable)

- Roles and responsibilities for the identified actions
- Time scales for the identified actions
- Levels of residual risks after the implementations of activities

2.6 Obtain Management Approval

The **[XYZ]** management should be kept informed about the overall progress and for every decision made. The data protection impact assessment report should be approved by the management and its accessibility by the public should be determined — either in full or in summarized form.

Signoff of the data protection impact assessment report should be in line with the documentation practices and policies of the **[XYZ]**.

a. Prior Consultation with the Supervisory Authority

According to the GDPR, the supervisory authority must be consulted prior to the processing of operations that have been identified as involving high levels of risk which cannot be mitigated by the controller.

The following information must be provided to the supervisory authority:

- Detailed responsibilities of the controller and processor
- Purposes of the processing
- Proposed activities to be implement to protect the personal data
- Contact details of the data protection officer (if applicable)
- A copy of the data protection impact assessment report

The supervisory authority should then provide a judgment on the processing and, if applicable, provide details on what must be done so the processing is acceptable under the GDPR requirements.

3. Conclusion

Data protection impact assessment is crucial for conducting a successful data-related project or activity and is a fundamental part of the GDPR. By having a clear understanding of the risks to the rights and freedoms of data subjects, **[XYZ]** should ensure that the current processes and controls can provide an appropriate level of data protection to the data subjects.

The data protection impact assessment process should ensure that **[XYZ]** is effectively managing and controlling risks that may affect its daily operations.