Data Protection Impact Assessment

Version 8

REZOLVE.ai

Document Information

Name of the document	Data Protection Impact Assessment
Release date	19-Dec-18
Owned by	Boopathi
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

VersionNo	VersionDate	Detailsof Change
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	15-Dec-2020	Review and no change
4	01-Dec-2021	Review and no change
5	04-Mar-2022	Updated Document Information
6	02-Mar-2023	Review and no change
7	28-June-2024	Updated Document Information
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	24-Mar-2025

Contents

ConsultSupervisoryAuthority7

1 Overview

The GDPR requires controllers to carry out Data Protection Impact Assessments ("DPIAs") in cases of potentially high-risk to the rights and freedoms of natural persons and to consult supervisory authorities ("SAs") in certain instances.
GDPR will rely on data controllers to assess the impact of envisaged data processing operations and only consult with SAs in relation to high-risk processing operations. In other words, if the data processing privacy risks cannot be mitigated lower than "High Risk", then SA need to be consulted.
Scope
The obligations to carry out DPIAs and consult with SAs in relation to high-risk processing operations directly apply to controllers only.
DPIA does not apply to situations in which Actionable Science is a processor. However, in such circumstances, the Company shall support the Data Controller in all ways to ensure that data processing is not at "High Risk" levels.

2 DPIA

DPIA Overview
A DPIA is an assessment of the impact of envisaged data processing operations on the protection of personal data, and more particularly an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from a processing operation.
Under the GDPR, controllers will be required to undertake DPIAs prior to data processing - in particular processing using new technologies - which is likely to result in a high risk for the rights and freedoms of individuals (Article 35).
DPIA that helps an organisation to identify privacy risks and ensure lawful practice when a new project is designed or changes are made to a service. The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is a particularly useful tool for organisations to identify privacy risks and ensure lawful practice use when:
Planning a new information sharing initiative such as working with new partners or in different ways;
Introducing new IT systems for collecting and accessing personal data;
Intending to use personal data for new uses.

Rights and Freedom of a person
The risk to the rights and freedoms of natural persons may result from personal data processing which could lead to physical, material or non-material damage, in particular:
where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data
economic or social disadvantage;
prevented from exercising control over their personal data;
where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, data concerning health or data concerning sex life
where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;

When is DPIA required
In line with the risk-based approach embodied by the GDPR, carrying out a DPIA is not mandatory for every processing operation. A DPIA is only required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons".
DPIA is required whenever personal data processing results in "High Risk" to rights and freedoms of individual. The GDPR text itself does not provide much guidance as to what would be considered a "high risk". Instead, it provides the following non-exhaustive list of cases in which DPIAs must be carried out:
Automated processing for purposes of profiling and similar activities intended to evaluate personal aspects of data subjects;
Processing on a large scale of special categories of data;
Systematic monitoring of a publicly accessible area on a large scale in case of large-scale processing operations which aim at processing considerable amounts of data and could affect a large number of individuals; or
As required by SAs which shall publish lists of processing operations which will fall under the DPIA requirement in Article 35(1), such as where data processing operations prevent data subjects from exercising a right or using a service or contract, or because they are carried out systematically on a large scale.

Examples of situations that require DPIA
A new IT system for storing and accessing personal data
A data sharing initiative where two or more organisations seek to pool or link sets of personal data
A proposal to identify people in a particular group or demographic and initiate a course of action
Using existing data for a new and unexpected or more intrusive purpose
A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system
A new database which consolidates information held by separate parts of an organisation
Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring
Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues

When is a DPIA not required
If Actionable Science has carried out a DPIA for a similar activity in the past, then a fresh DPIA is not required. Ie when the nature, scope, context and purposes of the processing are very similar to the processing for which DPIAs have been carried out. In such cases, results of DPIA for similar processing can be used

Contents of a DPIA
The GDPR does not formally define the concept of a DPIA as such, but its minimal content is specified by Article 35(7) as follows. (DPIAs shall contain at least the following information):
a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate interest pursued by the controller;
an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
an assessment of the risks to the rights and freedoms of data subjects that are likely to result from the processing (and in particular the origin, nature, particularity and severity of such risks); and
the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.

Other information to include in DPIA
Document the data flows in terms of, what data is being processed, where it is coming from and who it is going to
Clarify the legal basis
Identify and evaluate the privacy solutions (how can you reduce or remove the risk?)
Sign off and record the PIA outcomes
Integrate the outcomes into the project plan
Consult with internal and external stakeholders, as needed, throughout the process

Joint Controllers
When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities.

3 DPIA Procedures
Identification of Processes that require DPIA
For all new projects, applications and processes that involve personal data, the Project Manager shall consult Privacy Committee / DPO when carrying out DPIAs.
For all existing projects, applications and processes, a half-yearly review shall be conducted by DPO to determine if the privacy risk continues to lower than "High Risk"
Actionable Science shall assess whether their data processing activities are performed in compliance with any applicable DPIA, at least when there is a change of risk represented by the processing operations

Completion of DPIA
Complete the DPIA screening questions in Annexure A to determine if a comprehensive DPIA is required.
Complete the DPIA Template and related risk assessment for each project under DPIA scope.
DPIA Template
DPIA should be completed using the DPIA Templates (Word Document and Excel sheet). DPIA Template is attached as Annexure A (Word and Excel both)

Review and Approval of DPIA
The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation
Once it is determined that DPIA is required, the assessment shall be carried out using the DPIA Template
Completed DPIA shall be reviewed and approved by the Privacy Committee.
Data Processing that is part of the DPIA cannot continue or should not start until the approval is in place.

Records of DPIA
All DPIA shall be retained by DPO for future compliance purposes. Records will be made available to SA if requested

Consult Supervisory Authority
Actionable Science shall consult Supervisory Authority whether it can carry out or continue personal data processing when the following circumstances are present:
a DPIA status is "High Risk"
Existing or proposed controls cannot mitigate the risks to a level lower than "High Risk"

Procedure for Prior Consultation
Actionable Science needs to furnish the information below to make an application for consultation. All consultations shall be approved by CEO prior to sharing with the Regulators.
Purposes and means of the intended processing;
Measures and safeguards provided to protect the rights and freedoms of data subjects;
Contact details of the DPO
Copy of Data protection impact assessment (DPIA) performed that is triggering the prior consultation; and
Any other information requested by the SA.

4 Other Points
Fines
Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

NOTE - Next review cycle for this policy is March-2026. Management can review policy any time and can make changes depending on the situation.

- All documents related to policies and procedures any reference to Actionable Science is as good as Rezolve.ai