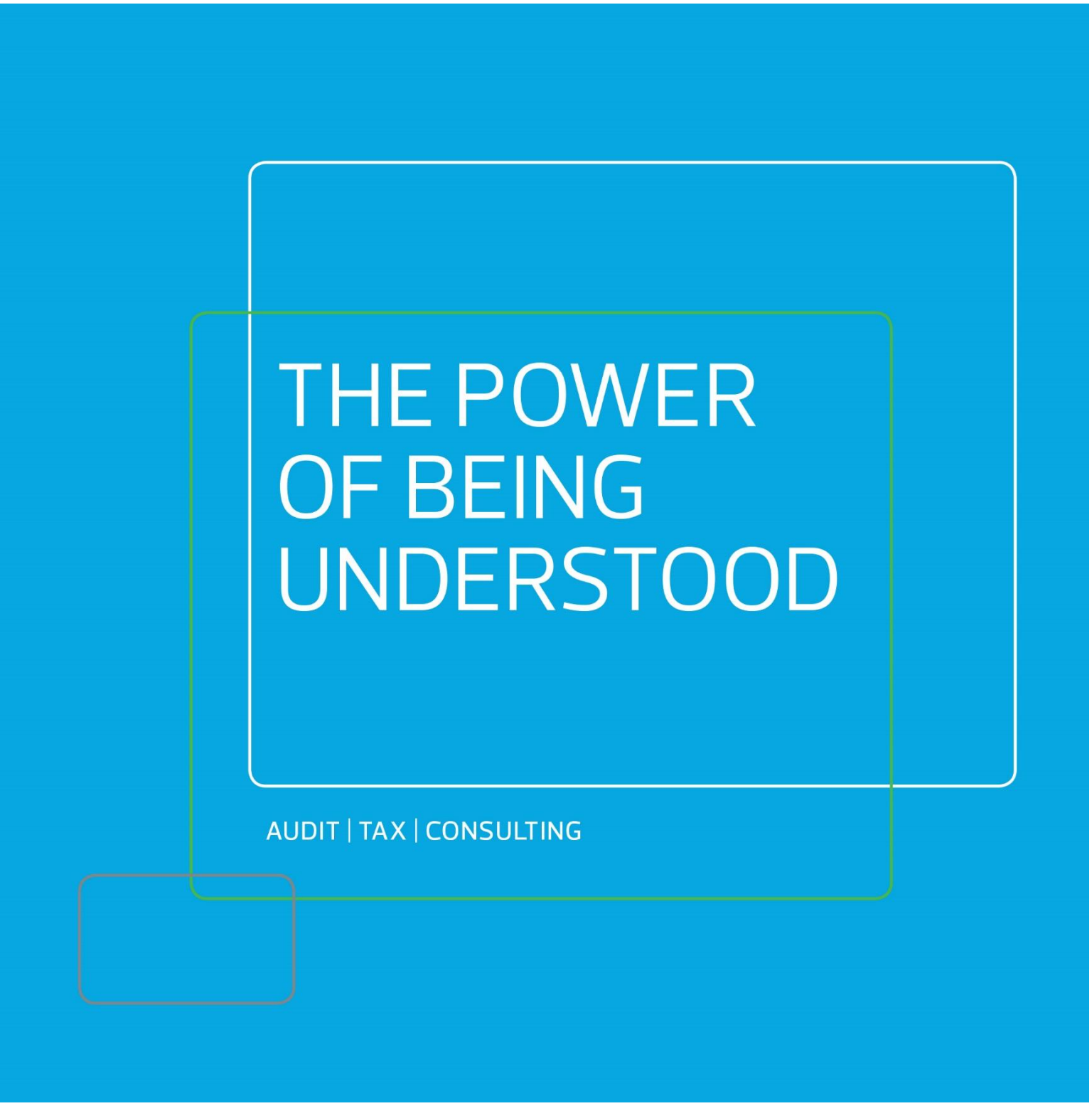


General Data Protection Regulation

A Guide to Conducting a Data Protection Impact Assessment

Contents

I. Introduction

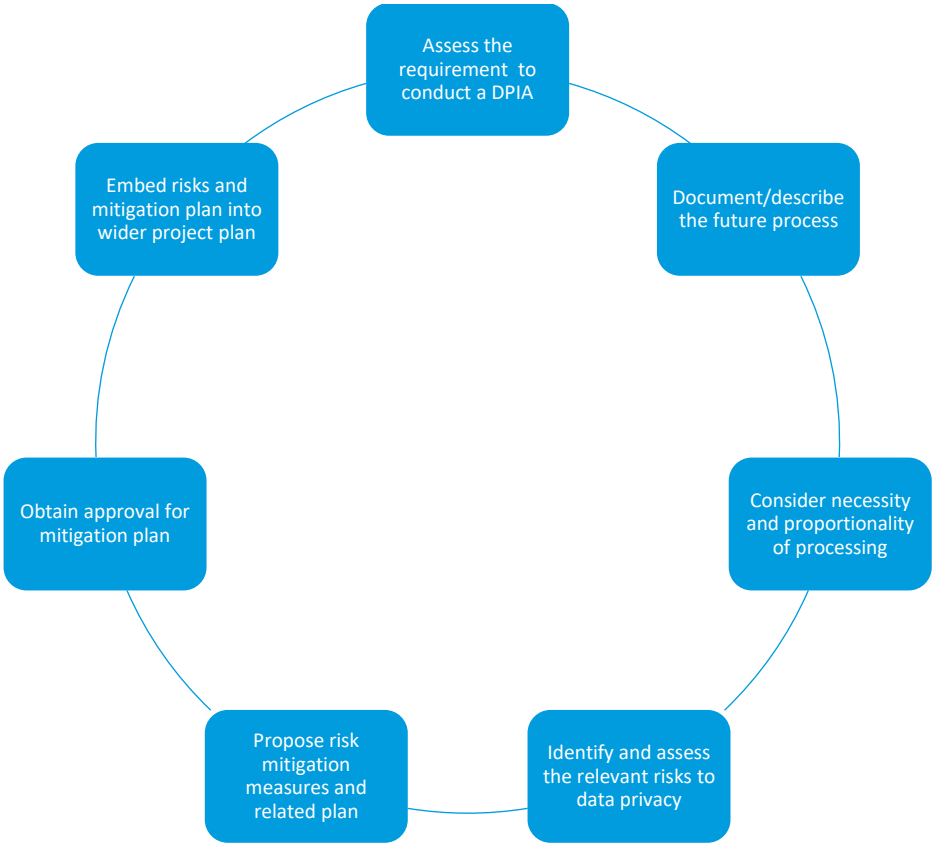
A Data Protection Impact Assessment (DPIA) is an exercise designed to assist organisations to consider, identify and minimise the data protection risks attaching to a new or existing project/process where the personal data of EU Citizens will be or is processed.

The General Data Protection Regulation (GDPR) introduced a requirement to undertake a DPIA, before engaging in processing, if the process is likely to result in a high risk to the personal data relating to an individual.

Hence, organisations need to ensure that their personnel are aware of the role of the DPIA, within the wider context of GDPR, and some staff will require training in the conduct of a DPIA. Hence, your entity is required to document an approach as to how your entity assesses the need for a DPIA to be undertaken. The methodology to be followed by personnel charged with completing a DPIA, if the initial review indicates a DPIA is required, also needs to be set out in a written format. It is likely that your key data protection policies will refer to DPIAs, as necessary, in indicating how, and when, your organisation should use DPIAs to boost compliance with both the GDPR and national data protection legislation.

A DPIA needs to be considered early in the life of any project which proposes to introduce any change to how, and what, personal data is processed – ideally during the planning phase of the project.

The key steps which underpin the successful conduct of a DPIA are set out below:



II. Assess the requirement to conduct a DPIA

A DPIA must be undertaken before you commence any processing which is likely to result in a high risk that the privacy of individual would be impacted either on a large scale or in a significant fashion.

The GDPR requires that you undertake a DPIA if it is planned to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

In addition, supervisory authorities, such as the Data Protection Commission, will expect that a DPIA is undertaken in circumstances where planned projects or activities feature some, or all, of the following characteristics:

- the use of new technologies;
- the use of profiling or special category data to decide on access to services;
- the profiling of individuals on a large scale;
- the processing of biometric or genetic data;
- the matching of data or the combining of datasets from varying sources;
- the collection of personal data from a source(s) other than the individual concerned without providing them with a privacy statement;
- the tracking of individuals' location or behaviour;
- the profiling of children or the promotion of online services to them; or
- the processing of data might endanger the individual's health or safety in the event of a security breach.

If a project includes any of the above elements, then a DPIA should be undertaken using a template such as the one that is set out below.

III. Data Protection Impact Assessment Template

DPIA requirement

[Insert a description of the background to the DPIA including the nature, scope, context and purposes of the process concerned].

A DPIA is required for the [insert name of process]:

Processing	Relevant criteria
Provide a brief description of processing What is the proposed legitimate basis for processing Is further processing undertaken?	Refer to the criteria within the Article 29 guidelines

Personal information

Personal data	Recipients	Period stored	Assets on which personal data relies

Consideration of relevant codes of conduct/policies

Code of Conduct/policy	Compliant (Yes/No)	Comment

Information Flow

[Insert relevant process maps and/or flows. Include risks as appropriate.]

Key process steps:

[A detailed step-by-step explanation of the above process map/flow to provide further insight to the relevant process. Highlight relevant risks.]

Necessity, proportionality and risk assessment

No.	Considerations	Comment	Risk to Individuals	Relevant Compliance Risk	Relevant Organisational Risk
1	Are there measures to ensure data collected is specific, explicit and legitimate in purpose?				
2	Are there measures to ensure data is processed lawfully? If consent is the legal basis to process personal data, are there measures to demonstrate consent? How is withheld or withdrawn consent managed?				
3	Are there measures in place to ensure data is not further processed in a manner inconsistent with the original purpose(s)?				
4	Are there measures to ensure data is adequate, relevant and limited to that which is necessary?				
5	Are there measures to ensure data is accurate and, kept up to date, where relevant?				

6	Are there measures to ensure data not retained for longer than is necessary for the purposes for which it is processed?				
7	Are there measures to provide relevant information (per GDPR Articles 12,13,14) to the data subjects?				
8	Are there measures to safeguard the data subject's rights of access and portability?				
9	Are there measures to safeguard the data subject's rights to rectify, erase, object and restrict processing?				
10	Are there measures in place to protect the rights of the data subject where data has been/will be disclosed to other recipients?				

11	Are there measures in place to protect the rights of the data subject where processing is carried out by a data processor?				
12	Are there technical and organisational measures in place to protect against unauthorised access to and/or the processing of personal data?				
13	Are there measures to ensure international transfers take place in a compliant manner?				
14	Are there measures in place to ensure consultation with the Supervisory Authority, if necessary, prior to the relevant process going 'live'?				

Actions to address data protection risks

The following table outlines the measures to address the privacy risks as outlined above.

Risk No.	Risk	Measure No.	Measures to address risk	Likelihood	Impact	Risk Rating	Evaluation: is the final impact on individuals represent justified, compliant and proportionate response?	Result (is the risk Eliminated, Reduced, Accepted, Gap Identified)
Risk number from above	Risk details from above	Measure No. (insert)	Details of any measures currently in place to address risk	Green, Amber, Red	Green, Amber, Red	Green, Amber Red	Evaluation of measures in place **Recommendation:** Recommendations and relevant actions to further address risk.	Residual risk

Required consultations

The below table outlines those individual or groups consulted during the preparation the DPIA.

Consultation group	Consulted (Y/N)	Detail
Data Protection Officer (DPO)		
Views of Data subjects or representatives of data subjects, where appropriate		
Supervisory Authority		

Approval of DPIA outcomes

[The following two tables summarise the actions required to address those data protection risks identified]

Risk No.	Approved Solution	Residual Risk Result	Approved By

Actions to integrate the DPIA findings back into the process

The below is a list of recommended actions which require incorporation into the process so as to integrate the DPIA findings.

Risk No.	Action No.	Action	Target completion date	Responsible individual

RSM Ireland
Trinity House
Charleston Road
Ranelagh
Dublin 6
Ireland

T: +353 (0) 1 496 5388
F: +353 (0) 1 496 926