

1. Introduction

Data Protection Impact Assessments (DPIAs) assist organisations to identify and minimise the privacy risks of new projects or policies, comply with their data protection obligations as well as to meet individuals' expectations of privacy. Data Protection laws (GDPR) require "privacy by design" to be at the heart of all activities which involve information about or that identifies people. Saving Faces demonstrates compliance with this requirement by conducting DPIAs. This is a formal approach to help us to properly identify and assess the risks to people from the way their personal data is collected, processed, shared, stored and disposed of. Saving Faces has a low appetite for the loss or breach of its business and stakeholder data in pursuit of its goals.

2. A DPIA must be conducted where processing is likely to result in a high risk to the rights and freedoms of individuals. This includes a number of specified types of processing and the screening checklist will help to determine when to do a DPIA. It is also good practice to conduct a DPIA for any other major project which requires the processing of personal data
3. Effective DPIAs are an integral part of taking a privacy by design approach allowing organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur. DPIAs can be used throughout the development and implementation of a project, using existing project management processes but can also be useful when an organisation is planning changes to an existing system.

To assess the level of risk, both the likelihood and the severity of any impact on individuals must be considered. High risk can result from a high probability of some harm, a lower possibility of serious harm or a combination of a moderate probability of a moderate level of harm.

4. Scope

All projects that involve high risk processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects are within the scope of this procedure and will be subject to a data protection impact assessment (DPIA).

5. Policy

- 5.1 DPIAs must be conducted where processing of personal data is likely to result in a risk to the rights and freedoms of individuals. For the purposes of this procedure, the processing of special categories of personal data is considered high risk processing of personal data.

DPIAs should always be completed when the processing involves:

- Processing of sensitive data (i.e. special-category or criminal-offence data) on a large scale;

- systematic monitoring of publicly accessible places on a large scale;
- use of innovative technology;
- profiling or special category data to decide on access to services;
- profiling of individuals on a large scale;
- processing of biometric or genetic data;
- matching data or combining datasets from different sources;
- collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing');
- tracking individuals' location or behaviour;
- profiling or targeting marketing at children; or
- processing data that might endanger the individual's physical health or safety in the event of a security breach.

If you are not planning on using personal information i.e. you are procuring hardware like a monitor or furniture, you do not need to complete a DPIA.

6. Screening

Saving Faces has developed a screening tool which asks a series of questions that will inform whether a DPIA will need to be completed. If you can answer yes to any of these questions, you may need to complete a DPIA. If in doubt, please contact the DPO.

- Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?
- Will the initiative involve the collection of new information about individuals?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Will the initiative require you to contact individuals in ways which they may find intrusive or outside of activities documented in our privacy notice?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Does the initiative involve you using new technologies including those which might be perceived as being privacy intrusive e.g. genetic data, photographs or fingerprints?
- Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Will the change or proposal use systematic and extensive profiling or

automated decision-making to make significant decisions about people?

- Do we intend to process special category data or criminal offence data on a large scale (big data)?
- Will we use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit?
- Will we combine, compare or match data from multiple sources?
- Will we process personal data in a way which involves tracking individuals' online or offline location or behaviour?
- Do we intend to process personal data which could result in a risk of physical harm in the event of a security breach?
- Systematic processing of sensitive data or data of a highly personal nature.
- Are we intending to handle data concerning vulnerable data subjects?
- Are we putting in place innovative technological or organisational solutions?
- Could what we are doing prevent people from exercising a right or using a service or contract?

7. Procedure

- 7.1 The Data Protection Officer or Project Manager identifies the need for a DPIA at the start of each project, assessing the project and type of personal data involved, or processing activity, against the screening questions set out in the DPIA tool.
- 7.2 Using the criteria below, following the likelihood and impact matrix, Saving Faces defines the risks to rights and freedoms of data subjects as:

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE

Document Control

Reference: DSP DOC 01-1.6.1a

Issue No: 2.1

Issue Date: 08/02/2023

Page: 4 of 7

Likelihood and impact matrix:

Likelihood	3	0	3	6	9
	2	0	2	4	6
	1	0	1	2	3
		0	1	2	3
		Impact			

Risks to rights and freedoms of data subjects:

Risk level	From	To	GDPR assessment
High	6	9	Highest unacceptable risk
Medium	3	5	Unacceptable risk
Low	1	2	Acceptable risk
Zero	0	0	No risk

8. Data processing workbook

- 8.1 Saving Faces captures the type of processing activity associated with the personal data being processed as part of the project. These are categorised as:
- Collection
 - Transmission
 - Storage
 - Access
 - Deletion
- 8.2 Saving Faces identifies the category of data processed, whether it is personal, special or that of a child, and the format of the data.
- 8.3 Saving Faces identifies who has access to the data (individuals, teams, third parties or data processor) or who are involved in the processing of personal data, or processing activity, recording the geographic location of where the processing takes place and / or if it is cross-border processing.

9. Identify privacy risks

- 9.1 Saving Faces assesses the privacy risks for each process activity as described in clause 7 above by:
- 9.1.1 Identifying and describing the privacy risk associated to that process activity.
 - 9.1.2 Using the likelihood criteria (1 – low, 2 – medium and 3 – high), scoring the likelihood of the risk occurring.
 - 9.1.3 Using the impact criteria (0 – zero impact, 1 – low, 2 – medium and 3 – high) of the risk should it occur.
 - 9.1.4 Producing a calculated risk, identifying the risk to the rights and freedoms of data subjects.
- 9.2 In assessing the privacy risks, Saving Faces considers risks to the rights and freedoms of natural persons resulting from the processing of personal data; risks to the business (including reputational damage); and its objectives and obligations (both regulatory and contractual).
- 9.3 Saving Faces identifies solutions to privacy risks, assigns a member of staff and sets a target date for completion.
- 9.4 Saving Faces prioritises analysed risks for risk treatment based on the risk level criteria established in clause 7.2 above.
- 9.5 Saving Faces risk owner, in consultation with Data Protection Officer, approves and signs off each DPIA for each data processing activity.

10. Prior consultation (Article 36, GDPR)

- 10.1 Where the DPIA identifies that processing of personal data will result in high risk to the data subject, in the absence of risk mitigating measures and controls, Saving Faces consults with the Information Commissioner's Office (ICO), using the following method.
- 10.2 When Saving Faces requests consultation from the ICO it provides the following information:
 - 10.2.1 Detail of the responsibilities of Saving Faces processor involved in the processing.
 - 10.2.2 Purpose of the intended processing.
 - 10.2.3 Detail of any/all measures and controls in place/provided to protect the rights and freedoms of the data subject(s).
 - 10.2.4 Contact details of the Data Protection Officer
 - 10.2.5 A copy of the DPIA.
 - 10.2.6 Any other information requested by the supervisory authority.

11. Responsibilities

- 11.1 The Data Protection Officer (DPO) must be consulted when completing a DPIA as they can advise whether a DPIA is needed, how you should conduct one, what measures and safeguards can mitigate risk, whether the DPIA has been done correctly and whether the processing can go ahead. The DPO will also monitor the processing to ensure that the actions planned have been implemented and that they are effective.
- 11.2 The Information Governance Lead is responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.
- 11.3 The Risk Owner is responsible for implementing any privacy risk solutions identified.

12. Document Owner and Approver

The Data Protection Officer is the owner of this document and is responsible for ensuring this procedure is reviewed.

A current version of this document is available to all/specified members of staff on the Saving Faces website.

This procedure was approved by Chief Executive Officer (CEO) and is issued on a version-controlled basis under their signature.

DATA PROTECTION IMPACT ASSESSMENT PROCEDURE


Document Control

Reference: DSP DOC 01-1.6.1a

Issue No: 2.1

Issue Date: 08/02/2023

Page: 7 of 7

Name	Iain Hutchison
Signature	
Approval Date	03/04/2024
Review Date	03/04/2025

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	IH	23 rd June 2021
2	Review, Addition of Introduction, Policy, Screening and amendments to Responsibilities	SM	22 nd June 2022
2.1	Defined charity's risk appetite in the introduction	FR	7 th February 2023
2.1	Reviewed – no changes	Hannah John and Ping San	13.02.2024