Data Protection Impact Assessment Policy

Document Ref No	DP-03
Version No	V1
Last review date	22/08/2022
Approved by	Harry Mongini
Next review	22/08/2023

Contents

1. Introduction

Faces Consent Limited (Faces) has a legal and ethical duty to protect and to avoid unnecessary interference with the privacy of individuals.

In order to carry out our services, we are required to undertake actions that may impact upon the privacy of:

- People who use the services we provide.
- Our own staff, and the staff of other organisations we work with.

It is vital that the likely impact of Faces actions upon the privacy of Data Subjects is understood and that the risks to privacy are robustly managed. Any interference with personal privacy must be minimised as much as possible and must be appropriate and proportionate.

To enable Faces to address the privacy concerns and risks, a technique referred to as Data Protection Impact Assessment (DPIA) must be used. This process ensures that we comply with the EU General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (DPA).

2. Purpose, scope and users

This policy applies to all Faces staff and activities where new personal data is being processed or personal data is being processed in a new way.

3. What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a way to systematically and comprehensively analyse the proposed processing of personal data and to help identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage.

A DPIA must:

- Describe the nature, scope context, and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

When assessing the risk, the likelihood and the severity of any impact on individuals must be taken into consideration.

4. When do we need a DPIA?

A DPIA must be done prior to the processing of any new personal data or the processing of personal data in a new way, this would include new projects and new processes – including:

- New IT systems for storing and accessing personal data
- Where data is shared with any other organisation
- A proposal to identify people in a particular group or of a particular opinion e.g. a survey
- Using existing data for a new and unexpected or more intrusive purpose
- The application of new technology to an existing system
- A new database which consolidates information held by separate parts of the business
- Transfers of services in or out of Faces e.g. cloud hosting

5. DPIA in practice

Managing data protection effectively and in line with legislation, current guidance and best practice is an important means of enabling the effective use of information for the benefit of our customers and for assuring all concerned that their information is managed safely and used appropriately.

All new projects, procedures and policies that involve using or sharing personal information will require a completed DPIA at the initial stages and prior to any procurement decision being made or any personal data being processed. The DPIA will be completed by the Project Lead.

The Project Lead must be in a position to influence the design and development of the and to participate fully in the projection design.

DPIAs will be managed and recorded via the Data Protection Impact Assessment. All information associated with the DPIA should be stored in a dedicated folder and titled with the relevant reference number (DPIA-001).

In the event of a breach of confidentiality or information security a DPIA and any associated information will be used as evidence in the investigation and may be requested by the relevant Data Protection Authority.

Any risks identified during the DPIA process must be managed in accordance with Faces Risk Assessment and Treatment Policy.

Where a high risk is identified and cannot be mitigated, Faces must consult the relevant Supervisory Authority. The Supervisory Authority will give written advice within eights (or fourteen weeks in complex cases). This advice should be followed as closely as possible.

6. Document management

Harry Mongini is responsible for the maintenance and accuracy of this policy. It must be reviewed and, if necessary, updated at least once a year. Notice of significant revisions shall be

7. Version Control

Summary of Change	Date of Change	Author	Version No
First Draft	22/08/2022	1T Compliance	1