University of Bedfordshire
Legal Office

Data Protection Impact Assessment Guidance

This document is intended to be used alongside the Data Protection Impact Assessment Form.

The General Data Protection Regulation (GDPR) 4 (e)6eGon rc1/e eat,(the (co(c)1 (controller rc)8 (ti)4c)2 shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A Data Protection Impact Assessment (DPIA) is a tool designed to help you identify and minimise the data protection risks of new projects. This is part of our accountability obligations under the GDPR, and a crucial component

Personal data: information relating to natural persons who can be identified or who are identifiable, directly from that information; or who can be indirectly identified from that information and other information. E.g. name, contact details, ID number, location data, online identifiers (including IP address).

Processing: any operation or set of operations performed on personal data, including collecting, organising, recording, structuring, storing, adapting/altering, retrieving, consulting, using, disclosing (e.g. by transmission, dissemination or otherwise), aligning or combining, restricting, erasing or destroying.

Processor: a natural or legal person, agency, public authority, or other body which processes personal data on behalf of a controller

Profiling: "Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements." (Article 4(4))

Pseudonymisation: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." (Article 4(5) GDPR)

Special category data: is personal data which is more sensitive and could create significant risks to a person's fundamental rights and freedoms, e.g. by putting them at risk of unlawful discrimination. This includes race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, or sexual orientation.

Step 1

Identify if a DPIA is needed

1) Always carry out a DPIA if you plan to:

☐ Use extensive and systematic profiling/automated decision-making to make key decisions about people.
Use profiling, automated decision-making or special category data to help you make decisions on someone's access to a service, benefit, or opportunity.
Carry out large scale profiling.
Carry out large scale processing.
Process the data of vulnerable data subjects.
Use new technologies.
Conduct large scale processing of criminal offence data or special category data.
Systematically monitor a publicly accessible place on a large scale.
Process genetic or biometric data
Compare, combine, or match data from multiple sources.
Process personal data without directly providing individuals with a privacy notice
Process personal data in a way which involves tracking people's online/offline behaviour or location
Process the personal data of children for profiling or automated decision-making or

for marketing purposes, or offer online services to them directly
Process personal data which could result in a risk of physical harm if there is a security breach
Process data in a way which prevents individuals exercising a right or using a service or contract
Participate in a new data

Step 4

Identify solutions/mitigations to the risks

8) Describe safeguards and security measures put in place, privacy by design, use of data processing and data sharing agreements.

9) Consider seeking the views of the data subjects, or their representatives and other interested parties (i.e. data processors, security specialists).

Step 5

Feed the results into the proposal

10) Assess if there are changes that need to be made to the proposal, and define how the risks will be monitored.

11) Make sure that the solutions proposed deal with the risk. If you are not sure about acceptable levels please contact the Data Protection Officer.

Step 6

Approval

12) Measures and residual risks should be approved by the relevant project lead. If any residual high risks are identified, the Data Protection Officer should be informed of these (as the ICO may need to be consulted).

13) Once completed, send the DPIA form to the Data Protection Officer, who will review it, and offer advice. It will then be sent for approval to the Senior Legal Officer, and Registrar.

Step 7

Implementation and Review

14) Once the DPIA has been approved, it is safe to proceed. Make sure that all those involved in the processing are aware of the necessary solutions.

15) Keep a record of your processing activities, and regularly review them to ensure they are still compliant with the acceptable position. Be responsive to any necessary changes.

16) Set review dates for 1 month, 3 months, 6 months, and then 12 months after the initial DPIA. Thereafter, review annually or if there is a change in how you process data (whichever is first). Inform the Data Protection Officer of any changes.