5 DATA PROTECTION IMPACT ASSESSMENTS

1. Purpose

Data Protection Impact Assessments (DPIAs) are a tool, described by the Information Commissioner as helping organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

Article 35 & 36 of the General Data Protection Regulation (GDPR) which came into force on 25 May 2018, resulted in the introduction of mandatory Data Protection Impact Assessments – DPIA.

This guidance note explains how a DPIA can assist you in ensuring that all privacy risks are considered when introducing new projects or making changes to existing services.

2. Definitions

A DPIA is a process which assists organisations in identifying and minimising the privacy risks of new projects or policies, or changes to existing services. Conducting a DPIA involves working with people within the organisation and with partner organisations to identify and reduce privacy risks. A DDPIA should benefit organisations by producing better policies and systems and improving the relationship between organisations and individuals.

The Information Commissioner's Office (ICO) has prepared a DPIA Code of Practice, explaining the principles that form the basis of a DPIA. The code sets out the basic steps for an organisation to follow during the PIA assessment process. This guidance note is made up of extracts from this code.

3. Benefits of a DPIA

Carrying out an effective DPIA should benefit the individuals affected by a project or introduction of a new service, and also the organisation carrying out the project.

A DPIA is often the most effective way to demonstrate to the ICO how personal data processing complies with GDPR.

The first benefit to individuals will be that they can be reassured that the organisations using their information have followed best practice. A project which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A second benefit to individuals is that a DPIA should improve transparency and make it easier to understand how and why their information is being used.

Organisations that conduct effective PIAs should also benefit, as the process of conducting the assessment will improve how they use information, which impacts on individual privacy. This should in turn reduce the likelihood of the organisation failing to meet its legal obligations and of a breach of the legislation occurring.

Conducting and publicising a DPIA will help an organisation to build trust with individuals using their services. The actions taken during and after the DPIA process can improve an organisation's understanding of their customers. There can also be financial benefits to conducting a DPIA, as identifying a problem early will generally require a simpler and less costly solution.

A DPIA can also reduce the ongoing costs of a project by minimising the amount of information that is collected or used where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of DPIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at the early stages of a project.

4. Projects which might require a DPIA

Article 35 and 36 of GDPR detail the specific requirements for a DPIA. It is a mandatory step in any new project particularly using new technologies where the processing is likely to result in high risk to the rights and freedoms of living individuals. Where there is a data protection officer they shall be consulted.

A DPIA is prescribed by GDPR where the business activity involves systematic and automated profiling, processing of large volumes of special category data, or systematic monitoring of a publicly accessible area on a large scale.

The core principles of DPIA can be applied to any project which involves the use of personal data, or to any other activity which could have an impact on the privacy of individuals.

DPIA terminology often refers to a project as the subject of a DPIA and this should be widely construed. A DPIA is suitable for a variety of situations:

- 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 (for example adding Automatic number plate recognition capabilities to existing CCTV);
- 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 use of information, or through surveillance or other monitoring.

A DPIA should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that DPIAs are more likely to be of use when applied to new projects or revisions of existing projects. Organisations should develop the capability to identify the need for a PIA at early stage and should consider building this into their project management or other business processes.

5. Screening for a PIA

Answering 'yes' to any of these questions below is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?

5 DATA PROTECTION IMPACT ASSESSMENTS

- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
- Will the project require you to contact individuals in ways which they may find intrusive?

For more detailed advice and a template DPIA, please refer to your organisation's Information Governance Lead and the ICO website and guidance:

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/