A practical guide to impact assessments

Nicola Fulford, Partner and Head of Data Protection and Privacy, and Krysia Oastler, Data Protection and Privacy Associate, Kemp Little LLP, provide practical advice on how to prepare for when PIAs become mandatory

Carrying out an impact assessment (also known as a privacy impact assessment, PIA, data protection impact assessment, risk assessment) as part of any new project involving personal data is currently a best practice requirement in Ireland. On 25th May 2018 when the General Data Protection Regulation ('GDPR') comes into force, PIAs will be mandatory in certain circumstances. This article gives guidance on undertaking impact assessments based on experience, the current published guidance and the new requirement in the GDPR.

The term 'new project' is used throughout this article to refer to any novel processing, including development and implementation of new technology, a different way of doing things or a material change to existing processes.

Background and best practice requirement

In terms of existing guidance, the European Commission's Privacy Impact Assessment Framework ('PIAF') project defines a PIA as 'a systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects'.

There are few publicly available Irish resources relating to privacy impact assessments, so some Irish organisations have been relying on guidance published by the UK regulator, the Information Commissioner's Office ('ICO'), which published its PIA Handbook in December 2007 (and has since published updates). In our experience, the ICO will ask the data controller whether an impact assessment was completed in relation to the processing activity.

In 2011, the Article 29 Working Party published a privacy and data protection impact assessment framework for RFID applications. Finally, the French regulator (the CNIL) published a comprehensive PIA manual in 2015, which includes a methodology, tools and good practices.

The momentum behind PIAs continued to build with the inclusion of impact assessments in the GDPR.

When is an impact assessment required under the GDPR?

Under the GDPR, it will be a legal requirement to complete a data protection impact assessment in certain 'high risk' circumstances. Such circumstances are defined in Article 35 of the GDPR as '*where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data'.*

The GDPR specifies that data controllers are in particular required to complete an impact assessment in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; and
- processing on a large scale of special categories of data/ sensitive personal data or systematic monitoring of a publicly accessible area on a large scale.

A single assessment may address a set of similar processing operations that present similar high risks.

Supervisory authorities are tasked with publishing a list of the kind of processing operations which are subject to the requirement for an impact assessment (and may also publish a list of processing operations that are not subject to the requirement).

Practical steps for carrying out an impact assessment

This section sets out some practical steps for carrying out an impact assessment.

Before going into the practical steps, and given that impact assessments are more effective when they are started early on in the development of a new project, how do you ensure that privacy is a consideration in the first place?

Training and awareness raising is a good place to start. However, having solid controls in place, such as privacy trigger points in existing project and risk management practices, is the best way to ensure that privacy is considered early on.

The ICO commissioned a study to understand how PIAs can be better integrated with existing project and risk management tools and how to make PIAs more practical and effective. The findings show that there are a number of places where the impact assessment process may be built into the main project and risk management practices.

For example, where the global PRINCE2 project management methodology is used, privacy could be built into the Business Case theme, the Organisation theme and the Risk theme. Other controls that I have witnessed involve building in a requirement to assess the need for a PIA into the remit of new project committees, legal review checklists, procurement processes and finance processes to ensure that any project involving the processing of personal data are captured.

> ***"It appears that the answer is not as simple as merely moving across from 'legitimate interests' to 'consent'. Instead, the solution may lie in responding to the overall move towards transparency and control, by evolving a two-way relationship with data subjects which engenders trust and secures more effective consents."***

The GDPR prescribes that the assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects; and
- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

1. Understanding and documenting personal data

The first step — and an ongoing one when completing a PIA — is to understand and document what personal data are being processed, why they are being processed (the purpose) and the data flows.

Some useful questions to ask as a starting point are:

- what personal data will be collected/ captured;
- why will this personal data be collected/captured;
- who will they be processed by (who will have access);
- who will they be shared with;
- where will they be processed and stored; and
- when will they no longer be needed.

These questions may be included in a form for project owners to complete at the beginning of the project, or as prompts for discussion in initial project meetings/privacy consultations.

Getting the answers to these questions can be challenging, as it involves working with many parts of the organisation and its suppliers/ subcontractors who may not be able to answer all of the questions at the beginning of the project.

2. Check legal compliance

Once you have an initial understanding of the project, the data flows and the purpose of the processing, the next step is to consider and check legal compliance. This is most effective when carried out early on in the project's life; it is an opportunity to structure the project in a legally compliant way.

Part of this step entails an assessment of the necessity and proportionality of the processing but also the other principles. For example, how the notice requirements are achieved, which condition(s) for processing are satisfied, how data minimisation will be applied, how individuals' rights will be fulfilled and the appropriate security measures needed to keep the data secure and confidential.

Any concerns regarding the legal compliance of the project should be raised and addressed early on. These may include building-in user-friendly, just-in-time notifications or icons to be transparent about processing, or functionality to provide data subjects with easy self-service access to their personal data.

3. Identify and assess privacy risks

The next stage is identifying and assessing privacy risks. Again, this

(Continued on page 8)

(Continued from page 7)

is an ongoing process (as the project develops, new risks may be identified and others may be avoided).

The ICO guidance takes a broad approach to identifying privacy risks, saying that organisations 'should identify any privacy risks to individuals, compliance risks and any related risks for the organisation; such as fines for non-compliance with legislation or reputational damage leading to loss of business'.

The GDPR requires an assessment of the risks to the rights and freedoms of data subjects. The CNIL described a privacy risk as '*a hypothetical scenario that describes how risk sources (e.g. an employee bribed by a competitor) could exploit the vulnerabilities in personal data supporting assets (e.g. the file management system that allows the manipulation of data) in a context of threats (e.g. misuse by sending emails) and allow feared events to occur (e.g. illegitimate access to personal data) on personal data (e.g. customer file) thus generating impacts on the privacy of data subjects (e.g. unwanted solicitations, feelings of invasion of privacy, etc.)'.*

An important part of the CNIL's approach is assessing the likelihood and impact should the feared event occur. This is important in practice, as the severity of the impact and the likelihood of the risk occurring will influence the measures that a controller takes to mitigate the risk. For example, it is unlikely that a controller would be expected to spend huge sums of money to mitigate a risk that is unlikely to materialise or that would have a limited impact if it did occur. See the CNIL's PIA Tools (templates and knowledge bases) for further guidance.

The ICO highlights the importance of consultation throughout the PIA process, and in particular when identifying privacy risks, to ensure that people with expertise in a relevant area are able to highlight risks and assess the likelihood and impact of the risk occurring. For example, the information security department should be consulted on the personal data security risks posed by a particular project and a sample of individuals whose data will be processed consulted on their views.

4. Consider ways of addressing risks

Once privacy risks have been identified, the next step is to consider ways of addressing them. Consultation with appropriate specialists at this stage will help to identify potential and pragmatic solutions to the risks.

To take a connected car as an example, you could include in the PIA a recommendation to build functionality into the in-car screen ('human machine interface') to display an icon providing notice to the driver when vehicle location tracking is on (to reduce the risk that an individual's journey is tracked without their knowledge).

Risks may be avoided completely (e.g. by not collecting certain types of personal data or changing the way that personal data are processed) or reduced to an acceptable level (e.g. by using anonymisation, pseudonymisation or implementing robust security measures).

In some cases, a controller may choose to accept the risk (because the likelihood of it occurring or the impact should the risk occur are minimal, or the risks of any potential harm can be managed such that they are outweighed by the benefits of the new project). In such cases, the project may go ahead as planned or with minimal changes. These considerations should be documented as well as the final decision on any actions that need to be taken. The decision maker(s) should also be documented as evidence of appropriate governance.

Where action needs to be taken, these tasks should be fed into a project plan or outstanding tasks list to ensure that they are tracked and completed. Note that impact assessments are never really complete and should be regularly reviewed and updated in light of any changes to the project or changes in the law and best practice. Controllers may choose to do this by diarising regular review milestones and establishing additional trigger points for review (such as material changes to the process and collection of new categories of personal data).

What next

It is clear that impact assessments are here to stay. And as the different approaches in the guidance available shows, there is no one right way of performing impact assessments: they are adapted to the project and the organisation.

However, there are some core common steps across the approaches to guide controllers on what they should be doing. How controllers decide to implement this will vary depending on the business and the existing project and risk management framework(s) that are already in place.

The GDPR permits a single assessment to address a set of similar processing operations that present similar high risks. As such, it is foreseeable that industry bodies may produce impact assessments for common processes. Further, privacy-conscious processors may decide to complete impact assessments for the technology they are selling to controllers as a value-add differentiator.

It is more efficient for a processor to complete one impact assessment on the technology it is selling than for hundreds of controllers to each complete a PIA and this would help the controllers purchasing their products. Finally, to help controllers, supervisory authorities are likely to produce more guidance on identifying and assessing privacy risks, particularly 'high risk' activities.

The Article 29 Working Party plans to issue guidance by the end of 2016 on high risk processing and data protection impact assessments.

Nicola Fulford and Krysia Oastler
Kemp Little LLP
nicola.fulford@kemplittle.com
krysia.oastler@kemplittle.com