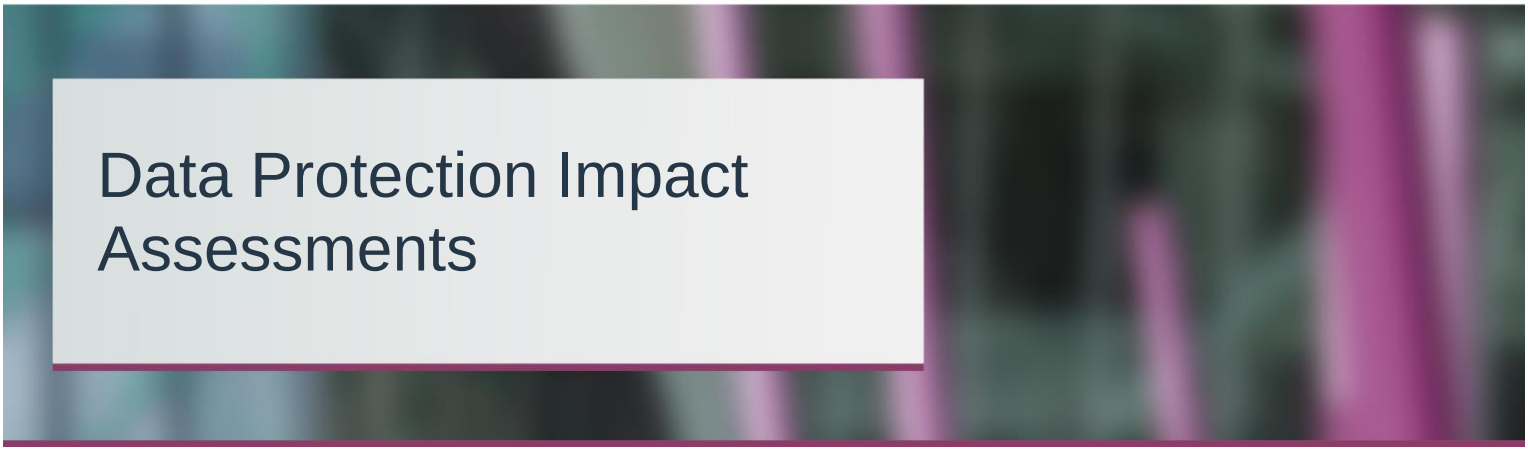
WILLIAM FRY

// PRIVACY SOURCE



Data Protection Impact Assessments

Data Protection Impact Assessments (**DPIAs**) are the EU General Data Protection Regulation's (**GDPR**) toolkit for organisations to identify, address and minimise any data protection risks in processing, in particular when using new technologies.

A DPIA is a process specific mechanism for organisations to apply at the **development and design phase** of any project in which personal data will be processed. A DPIA is to be used to ensure that real and systematic efforts are made to **fully assess the impacts and any data protection risks to** individuals in the collection, use and disclosure of their personal information in a project. The end- goal is for: (1) data protection and privacy impacts to be assessed; and (2) risks to be identified, in each case with a view to mitigation by prospectively implementing privacy-enhancing solutions and to seek to prevent non-compliance. DPIAs are a core tool in **Data Protection by Design** – a theme which flows throughout the GDPR.

Data Protection by Design

A high priority objective of the GDPR is for data protection to be the norm in all organisations. The GDPR aims for data protection to be at forefront of all projects from the outset and for it to be designed into all actions undertaken by an organisation that involve processing activities. A DPIA is a mechanism for organisations to use in order to design data protection and privacy measures into their processing activities.

Significant impact

In practice, DPIAs are not new. Many organisations will be familiar with the process of DPIAs under the guise of privacy impact assessments. A key factor under the GDPR is that it removes the voluntary nature of conducting DPIAs as they are written into law and mandated for in the circumstances in which it is required of a controller to conduct a DPIA.

The GDPR facilitates organisations in understanding **when to conduct a DPIA**. In addition, the GDPR, and guidance from national Supervisory Authorities (**SAs**), guides organisations on the **DPIA process**. Data Protection by Design and Default and DPIAs have a significant impact on data protection compliance.

When to conduct a DPIA

Many processing activities are now the subject of mandatory DPIAs rather than a voluntary measure of best practice and compliance.

The circumstances in which it is mandatory to conduct a DPIA are:

- where an organisation is developing or designing a new product, service, policy, business initiative or technology that is ***likely*** to result in ***a high-risk*** **to the rights and freedoms of individuals** (in such circumstances, the DPIA must be conducted before the project is implemented);

- where processing activities involve the systematic and extensive evaluation of personal aspects based on **automated processing** including profiling, and on which decisions are based that **produce legal or other significant effects;**
- where processing is on **a large scale of special categories** of data (e.g. race, health) or data relating to **criminal convictions and offences**;
- where processing involves the **systematic monitoring of a publicly accessible area on a large scale.**

Benefits of a DPIA

From a compliance perspective, a DPIA is one of the most effective mechanisms to demonstrate an organisation's technical, organisational and systematic compliance with data protection laws. By analysing the data that an organisation processes and understanding the associated risks an organisation will automatically improve the quality of data processed (including by data minimisation) and reduce or eliminate any non- compliance risks.

From an organisational perspective, a DPIA demonstrates that data protection and protecting the fundamental rights and freedoms of data subjects is a high priority in an organisation. It shows that the organisation is transparent in its data protection practices and therefore it is one to be trusted by customers/clients with their personal data.

DPIA process

The DPIA process essentially involves a balancing test being conducted by an organisation in relation to the impact of the processing activities, of the proposed project, on the privacy rights of individuals concerned and whether it would result in an unwarranted prejudice to or intrusion on these rights. The level of risk will need to be assessed.

While the process of conducting a DPIA appears to be flexible, the GDPR is prescriptive in relation to what a DPIA assessment must include. According to the GDPR, a DPIA must contain and document at least the following:

A systematic description of the envisaged processing (i.e. a description of the proposed project)

The *purposes* of the processing, including any legitimate interest of the organisation as the data controller

An *assessment of the necessity* for the proposed processing and the degree of proportionality in such processing

An *assessment of the risks* to the data subjects' rights and freedoms

The measures envisaged to address the risks including safeguards, security measures and mechanisms to ensure protection of data and compliance with GDPR

In order to collate the information mandated, it is clear that organisations can do so in many ways including by way of consultation with stakeholders and coordinating organisational workshops.

Where a *processor* is engaged by a controller, the GDPR requires the processor to assist the controller in the DPIA process taking into account the nature of the processing and the **information available** to the processor.

A novel aspect of DPIAs under the GDPR is that, where appropriate, an organisation can seek the views of data subjects on the intended processing.

What happens if a DPIA identifies "likely high-risk" processing?

In the event that a DPIA identifies that a project involves "likely high-risk" processing, an organisation must consult with its national SA. In its Guide to Data Protection Impact Assessments published October 2019, the Irish SA, the Data Protection Commission (DPC), advise that it is not necessary to contact the DPC where appropriate measures are identified in the DPIA which would sufficiently mitigate the risks presented by the processing. The DPC acknowledge that, in almost all cases, it will not be possible to eliminate data protection risks completely, but a DPIA assists controllers balance those risks against the aims of a given project, to ensure that any risks that are accepted are proportionate to the outcomes of the project. However, where a DPIA does not identify safeguards which effectively mitigate any residual high risk, the DPC must be consulted before the project moves forward.

If the project goes ahead, then a DPIA will assist in demonstrating that an organisation has complied with its data protection obligations. In addition, if a complaint is received from a data subject, the DPIA will evidence that the organisation had adequately balanced the legitimate interests of the organisation against the privacy rights of the individual making the compliant (subject, of course, to the DPIA being within sufficient scope of the complaint).

Conclusion

In today's evolving digital era, organisations are constantly creating new products and services that will involve processing activities. The ways in which personal data can be captured, used, monitored and analysed are ever increasing. DPIAs offer benefits to organisations by balancing the privacy rights of individuals with the objectives of the organisation and evidencing good data protection compliance. The DPIA process aims to identify and minimise data privacy risks. Most importantly however, DPIAs benefit data subjects by protecting their fundamental rights and freedoms, ensuring the least privacy-intrusive product or service is offered to them.

The shift from DPIAs being a voluntary measure of best practice to a mandatory step that must be carried out in the context of a *"likely high-risk"* processing activities add to the layers of accountability and documented compliance under the GDPR. Certainly, the nature and scope of a DPIA will be commensurate to the scale of the project or type of processing. The objective of the GDPR in mandating DPIAs is to incorporate a Data Protection by Design approach in all organisations and to prompt them to consider a project from the perspective of data subjects, not just from an economic perspective.

Contact Us

If you have any queries in relation to this, or would like to know more about our PrivacySource offering, please contact our Partner below, or your usual William Fry contact.

David Cullen
PARTNER
+353 1 639 5202
david.cullen@williamfry.com

Leo Moore
PARTNER
+353 1 639 5152
leo.moore@williamfry.com

John O'Connor
PARTNER
+353 1 639 51823
john.oconnor@williamfry.com

Contact our PrivacySource Team here

Follow us @WFIDEA