BRODIES LLP

GDPR - CARRYING OUT **PRIVACY IMPACT ASSESSMENTS**

Under the General Data Protection Regulation (GDPR), data protection impact assessments (DPIAs or PIAs) are mandatory for certain types of processing. This guide explains what a DPIA is and when they should be used.

What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process to help organisations identify, assess and mitigate or minimise privacy risks with data processing activities – for example, the launch of a new product or the adoption of a new practice or policy or system. It is also relevant to decisions to, for example, outsource a service or function to a third party or to undertake internal reorganisations (for example, the centralisation of an HR function or IT systems in a multinational business).

A DPIA is an integral part of privacy by design, and is a key component in helping an organisation to comply with its obligation to demonstrate with the GDPR. A DPIA should set out:

- a description of the envisaged processing operations and the purposes of the processing
- an assessment of the necessity and proportionality of the processing
- an assessment of the risks to the rights and freedoms of data subjects
- the measures envisaged to address the risks and demonstrate compliance with the GDPR

Organisations should have appropriate policies in place within their organisations to ensure that a DPIA is considered in relation to any new processing activities and, where a DPIA is to be performed, how it will be carried out.

Guidance from the Article 29 Working Party (WP29) sets out criteria that organisations can use to assess whether or not a DPIA, or a methodology to carry out a DPIA is sufficiently comprehensive to comply with the GDPR.

When must an organisation undertake a DPIA?

The GDPR requires that organisations carry out a DPIA where the processing is likely to result in a "high risk" to the rights and freedoms of data subjects. The obligation to conduct a DPIA is on the data controller.

The GDPR expressly references the use of new technologies, systematic and extensive evaluation using automated processing, large scale processing of special category (sensitive) personal data and "systematic monitoring of a publicly accessible area on a large scale" as examples of things that might constitute high risk processing. The DPIA should be carried out prior to commencing the processing.

The WP29 guidance expands on this to give some non-exhaustive examples such as credit monitoring, genetic testing, the use of communications or location data, matching or combining datasets, processing data concerning vulnerable data subjects (such as employees), and using innovative technology such as fingerprint recognition.

However, given the benefits, the WP29 also emphasises that a DPIA should be considered whenever an organisation is considering a new project and if the organisation decides not to carry out a DPIA then it should document why.

Do I need to carry out a DPIA for existing processing activities?

No – unless there is a material change in risk. The WP29 recommends that DPIAs are regularly reviewed (at least every three years), you should therefore plan to carry out a DPIA for existing activities in due course.

When should a DPIA be carried out?

As early as possible in relation to any new project, so that its findings and recommendations can be incorporated into the design of the processing operation. Organisations should also revisit their DPIAs as a project progresses, the issues identified and risk mitigation plans to ensure that they remain up to date.

Who should be involved in producing a DPIA?

If an organisation has a Data Protection Officer (DPO), then the DPO should play a key role in carrying out a DPIA. The WP29 expects that organisations will seek the advice of the DPO and document that, and the decisions taken, in the DPIA.

Where data is being processed by a data processor, the processor should assist the controller in carrying out the DPIA – for example by providing information on the processor's practices and systems.

Finally, the GDPR requires organisations to "where appropriate" seek the views of data subjects and their representatives. The WP29 suggests that consultation could be done in a number of ways – for example:

- an internal or external study
- in the case of employees, formal consultation with staff representatives/unions
- in the case of customers/consumers, a survey sent to prospective customers

The WP29 considers that if organisations decide not to consult with data subjects then they should document why. They should also document the outcome of the consultation, including the reasons for any decision that differs from the views expressed by data subjects.

Is there any requirement to consult with the ICO?

If a DPIA indicates that processing would result in a high risk, and it is not possible to adopt measures to mitigate those risks, then the GDPR requires that organisations consult with the relevant supervisory authority (in the UK, the ICO).

The WP29 gives the example of a proposal to store personal data on laptop computers. If the organisation adopts appropriate data security measures (for example, full disk encryption, access control and secured back-ups), then the risks will have been mitigated and there would be no need to consult with the relevant supervisory authority.

More information

You can follow the latest developments on the GDPR, including the latest guidance from regulators, on our GDPR microsite:

brodies.com/GDPR

or our blog:

http://techblog.brodies.com

Is there an obligation to publish DPIAs?

In line with the transparency obligations under the GDPR, the WP29 recommends that organisations consider publishing their DPIAs – either in full or by way of a summary. The WP29 emphasises that publishing a DPIA can be helpful in fostering trust, particularly where the processing affects members of the public.

Where can I find the WP29's draft guidance on DPIAs?

The draft guidance can be downloaded from the WP29 website.

Key contacts

Grant Campbell
PARTNER
+44 (0)131 656 0115
grant.campbell@brodies.com

Martin Sloan
PARTNER
+44 (0)131 656 0132
martin.sloan@brodies.com

Christine O'Neill
PARTNER
+44 (0)131 656 0286
christine.oneill@brodies.com

Charles Livingstone
PARTNER
+44 (0)131 656 0273
charles.livingstone@brodies.com