Data Protection Impact Assessment under the GDPR

The GDPR will require controllers to carry out Data Protection Impact Assessments ("DPIAs") in cases of potentially high-risk processing activities and to consult supervisory authorities ("SAs") in certain instances.

A positive side effect of the introduction of DPIAs will be the abolishment of the general obligation to notify data processing operations to SAs. Rather than generally requiring the notification of data processing operations to SAs (as is currently required in most EU countries), the GDPR will rely on data controllers to assess the impact of envisaged data processing operations and only consult with SAs in relation to high-risk processing operations.

1. Key Takeaways
   (a) Where a type of data processing is likely to result in a high risk for the rights and freedoms of individuals, controllers shall carry out a DPIA prior to the processing to assess the impact of the envisaged processing operations on the protection of personal data.
   (b) The GDPR text itself does not provide much guidance as to what would be considered a "high risk" for the rights and freedoms of individuals. But it does provide a non-exhaustive list of examples as to when DPIAs will be required and further guidance from SAs can be expected.
   (c) The GDPR does not prescribe the process for undertaking DPIAs. Existing or future SA guidance on conducting DPIAs will be the best source of guidance.
   (d) If a DPIA carried out by a controller indicates that an envisaged processing would result in a high risk in the absence of risk-mitigating measures taken by the controller, the controller shall consult the SA prior to the processing.
   (e) The obligations to carry out DPIAs and consult with SAs in relation to high-risk processing operations directly apply to controllers only. But processors should assist controllers, where necessary and upon request, in complying with these obligations.

2. DPIAs
   (a) What are DPIAs and when must they be undertaken?

A DPIA is an assessment of the impact of envisaged data processing operations on the protection of personal data, and more particularly an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from a processing operation.

Under the GDPR, controllers will be required to undertake DPIAs prior to data processing - in particular processing using new technologies - which is likely to result in a high risk for the rights and freedoms of individuals (Article 35). The GDPR provides the following non-exhaustive list of cases in which DPIAs must be carried out:

- automated processing for purposes of profiling and similar activities intended to evaluate personal aspects of data subjects;
- processing on a large scale of special categories of data or of data relating to criminal convictions and offences;
• systematic monitoring of a publicly accessible area on a large scale.

Recital 91 further indicates that DPIAs will need to be undertaken:

• in case of large-scale processing operations which aim at processing considerable amounts of data and could affect a large number of individuals; or

• as required by SAs which shall publish lists of processing operations which will fall under the DPIA requirement in Article 35(1), such as where data processing operations prevent data subjects from exercising a right or using a service or contract, or because they are carried out systematically on a large scale.

(b) Scope of DPIAs

DPIAs shall contain at least the following information:

• 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 that are likely to result from the processing (and in particular the origin, nature, particularity and severity of such risks); and

• the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.

The GDPR does not prescribe any process or format for DPIAs. For the time being, existing guides on conducting DPIAs issued by local SA will likely be the best source of guidance.

(c) Existing processing operations

Interestingly, the GDPR is silent on whether the DPIA requirement will apply in relation to processing operations already underway once the two-year transition period finishes and the GDPR provisions start to apply. Strictly speaking, DPIAs must be undertaken before processing operations start which will be impossible in relation to ongoing processing operations. On the one hand, it seems rather burdensome to expect organisations to assess all of their existing processing operations as to whether they need to be subjected to a DPIA under the GDPR, and then carry out DPIAs, as required. On the other hand, turning a blind eye to existing processing operations and only require DPIAs in relation to processing operations that start following the transition period also does not seem appropriate. In the absence of further guidance on this point, we would recommend as a best practice approach that organisations identify all of their key, long-term risky processing operations (including ongoing ones) and, subject to providing time for supervisory authorities to publish further guidance, undertake DPIAs in relation to them.

(d) Other points to note regarding DPIAs

The following other points are noteworthy:
Where a set of similar processing operations present similar high risks, a single DPIA may be undertaken to address all of those processing operations. In this regard, Recital 92 provides the example of several controllers planning to introduce a common application or processing environment across an industry sector or segment for a widely used horizontal activity.

Controllers must seek the advice of their DPO (if any) when carrying out DPIAs.

Compliance with approved codes of conduct shall be taken into account when assessing the impact of processing operations and may well have a risk-minimising effect.

Without prejudice to the protection of commercial or public interests or the security of processing obligations, where appropriate, controllers shall seek the views of data subjects (or their representatives) on any intended processing. It remains to be seen in which cases data subjects' views should be sought.

Controllers shall assess whether their data processing activities are performed in compliance with any applicable DPIA, at least when there is a change of risk represented by the processing operations.

3. Prior consultation procedure

If a DPIA carried out by a controller indicates that an envisaged processing would result in a high risk in the absence of risk-mitigating measures taken by the controller, the controller shall consult the SA prior to the processing (Article 36). Recital 94 seems to slightly soften this requirement by providing that a consultation might not be required if the controller is of the opinion that the identified risk can be mitigated by reasonable means in terms of available technologies and costs of implementation.

If the SA considers that the processing in question would infringe the GDPR, the SA should respond to such requests within eight weeks. However, the eight week period may be extended by six weeks in complex matters and may also be indefinitely suspended until the SA has obtained all information requested for the purposes of a consultation. Consequently, the consultation process may take considerably longer than the projected eight week period. Further, Recital 94 clarifies that a lack of response from an SA within the defined period will not preclude an SA from exercising its powers, such as the power to prohibit processing operations. Hence, a lack of response to a consultation request does not confirm that an envisaged processing is GDPR-compliant nor does it mean that SAs will not take action against such processing. This might lead to considerable uncertainties in practice.

As part of the prior consultation process, a controller must furnish the following information to the SA:

- where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- the purposes and means of the intended processing;
- the measures and safeguards provided to protect the rights and freedoms of data subjects;
- the contact details of the DPO (if applicable);
- the data protection impact assessment triggering the prior consultation; and
- any other information requested by the SA.
4. Your DPIA Game Plan

DPIAs will play an important role under the GDPR. The Art. 29 Working Party announced in February that - as a matter of priority - that it will issue (much needed) guidelines or processes on the notion of high risk and DPIAs to help controllers and processors get prepared for the GDPR.

Controllers should take seriously their obligation to carry out DPIAs and we recommend the following steps:

- establish guidelines for what would constitute risky processing operations that will likely require closer scrutiny by way of a DPIA;
- establish policies, processes and templates for carrying out DPIAs and consider how DPIAs can be embedded within the organisation's operational strategy;
- consider what training programmes, threshold analyses and escalation mechanisms are required to allow individuals with access to personal data to be in a position to express their views as to whether a DPIA should be carried out;
- review key (ongoing and planned) data processing operations and identify those that will be subject to the DPIA requirement;
- start carrying out DPIAs as a matter of best practice;
- consider signing up to relevant codes of conduct that might reduce the need for DPIAs; and
- establish processes for consulting with SAs in relation to high-risk processing operations.

* * * * *

Please contact your usual Baker & McKenzie contact for assistance in preparing policies, guidelines and templates for carrying out DPIAs, for implementing related processes and for assessing your organisation's processing operations in light of the new requirements.