GDPR series: demystifying DPIAs

Samantha Sayers, Solicitor, and Kayleigh Clark, Senior Associate, PricewaterhouseCoopers LLP, explain how to meet the GDPR's requirements for carrying out DPIAs

To date, Privacy Impact Assessments have been widely recognised as a valuable, but not mandatory, tool that organisations can use to assess and reduce the privacy risks associated with their personal data processing activities. Some of the EU data protection authorities, including the UK Information Commissioner's Office ('ICO') and France's Commission Nationale de l'Informatique et des Libertes ('CNIL'), have issued codes of practice recommending the use of PIAs, and setting out methodologies. However, there has been no industry-wide methodology for performing PIAs, with the result that organisations have found it challenging to know where to begin.

The General Data Protection Regulation ('GDPR') coming into effect in May 2018 introduces for the first time the legal requirement for all organisations to carry out 'Data Protection Impact Assessments' ('DPIAs') where their personal data processing activities are likely to result in 'high risk' to individuals. But the same questions remain as to exactly what form the DPIA should take, and how it should be conducted.

This article aims to shed some light on the scope of the new GDPR requirements and highlights some practical aspects to consider when completing DPIAs.

What are DPIAs supposed to do?

DPIAs are internal assessments organisations carry out in order to help them to identify the potential effects on individuals' privacy, as well as legal and compliance implications, of any new or existing data processing. They are often undertaken prior to implementing a new project, business process, system or application.

The ICO's Code of Practice states that 'an effective PIA will allow organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur'. But essentially the core purpose of a DPIA is to identify risks arising from personal data processing and identify adequate measures to reduce these risks.

Changes under the GDPR

Article 35(1) of the GDPR introduces a new requirement for organisations to carry out a DPIA prior to undertaking data processing activity 'where a type of processing in particular using new technologies...is likely to result in a high risk to the rights and freedoms of natural persons'. The GDPR also requires the DPIA to be carried out prior to the data processing being undertaken. Accountability for ensuring that DPIAs are performed lies with the data controller. The DPIA may be conducted by someone else, whether internal or external to the organisation, but the data controller remains ultimately responsible for the completion of the DPIA.

Article 36 of the GDPR contains the new requirement for organisations to consult with the relevant supervisory authority prior to undertaking processing where a DPIA has indicated the processing would result in a high risk to individuals. Where the supervisory authority decides that the intended processing is likely to infringe the GDPR, the supervisory authority must provide written advice to the data controller within 8 weeks (which may be extended by a further 6 weeks in the case of complex processing activities). The supervisory authority may use any enforcement powers available to it under Article 58 to mitigate the risks identified by the DPIA.

In addition to the Article 35 DPIA requirement for assessing high risk processing, organisations need to understand the interplay with Article 24 of the GDPR concerning the overall responsibility of the data controller in respect of its personal data processing activities. Article 24 presupposes that risk assessments should be an intrinsic part of a data controller's personal data processing activities, and that the risks to individuals should always be considered. In order to achieve this, the data controller should create processes that work not just legally, but operationally in order to deliver meaningful and measurable change. There needs to be a linear path between an organisation's Article 35 DPIA framework and the Article 24 risk assessment requirements, which is important to get right

(Continued on page 4)

(Continued from page 3)

for process design. This is discussed in further detail below.

How do you determine if the risk is 'high risk' enough to require completion of a DPIA?

As mentioned above, the requirement to carry out a DPIA does not apply to all data processing activities. A DPIA is only required where the type of processing, particularly those using new technologies, is likely to result in a high risk to individuals.

In determining whether the processing is high risk enough to trigger the requirement for an Article 35 DPIA, the data controller must first assess the likelihood and severity of the risks associated with the processing activity as required by Article 24(1). Risk assessments are an intrinsic part of the GDPR, and a DPIA is a way of assessing the likely risks to individuals, and for identifying the measures that need to be implemented to comply with the GDPR's accountability requirements.

To help organisations determine whether the processing is 'high risk', Article 35(3) provides a non-exhaustive list of examples where a DPIA is required, which includes:

- where the processing involves a systematic and extensive evaluation of personal aspects relating to individuals, which is based on automated processing including profiling, and on which decisions are based that produce legal effects concerning the individuals;
- where there is processing on a large scale of special categories of data or of data relating to criminal convictions and offences; or
- where the processing involves a systematic monitoring of a publicly accessible area on a large scale.

> ***"In cases where it is unclear whether a DPIA is required, the Working Party recommends that a DPIA is carried out nonetheless, as a DPIA is a useful tool to help data controllers comply with data protection law. In addition, as a matter of good practice, the Working Party recommends that a DPIA should be re-assessed at least every 3 years, to ensure that the risks to individuals continue to be mitigated."***

However, as this list is non-exhaustive, there may be processing operations that are not captured, but which pose similarly high risks and should also be subject to DPIAs. The Article 29 Working Party has recently issued guidance on DPIAs ('Guidelines', copy at: www.pdpjournals.com/docs/88687) which further sets out examples of processing 'likely to result in a high risk', which includes the following:

- evaluation or scoring, including profiling and predicting, of data subjects;
- automated-decision making with legal or similar significant effect;
- systematic monitoring;
- processing of sensitive data;
- data processed on a large scale;
- datasets that have been matched or combined;
- data concerning vulnerable data subjects;
- innovative use or applying technological or organisational solutions;
- data transfer across borders outside the European Union; and
- when the processing in itself prevents data subjects from exercising a right or using a service or a contract.

As a general rule, the Article 29 Working Party advises that where a processing activity meets at least two of the criteria listed above, then a DPIA will be required. However, it depends on the specific processing activity, as it may be enough for only one of the criteria to be met in order to justify the completion of a DPIA.

Where the data controller determines that the processing is not high risk, despite satisfying two of the criteria, then the Working Party recommends that the data controller fully documents its reasoning for not completing a DPIA. In cases where it is unclear whether a DPIA is required, the Working Party recommends that a DPIA is carried out nonetheless, as a useful tool to help data controllers comply with data protection law. In addition, as a matter of good practice, the Working Party recommends that a DPIA should be re-assessed at least every 3 years, to ensure that the risks to individuals continue to be mitigated.

What should the DPIA contain?

Once organisations have determined that an Article 35 DPIA is required, the GDPR also sets out some minimum requirements as to the content of a DPIA. These requirements are summarised as follows:

- a systematic description of the envisaged processing operations and the purposes of the processing including which legitimate interest is being pursued (where applicable);
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes for which the person-

al data are collected;

- an assessment of the risks to the rights and freedoms of the data subjects impacted by the processing; and
- the measures envisaged to address the risks, including which safeguards, security measures and mechanisms will be employed to protect the personal data processed.

Provided the DPIA contains the elements set out above, the actual format and implementation of the DPIA is up to the data controller.

What information needs to be provided to the supervisory authority?

Where organisations have conducted DPIAs which have identified high risk processing activities, they must also ensure that they provide the following information to the supervisory authority:

- the responsibilities of the parties involved (i.e. controller, joint controllers and processors) in the processing;
- the purposes and means of the intended processing;
- the measures and safeguards in place to protect the rights of data subjects;
- the contact details of the Data Protection Officer (where applicable);
- a copy of the DPIA carried out; and
- any other information requested by the supervisory authority.

The requirement to consult with the supervisory authority is likely to result in a higher administrative burden, not just for organisations undertaking the DPIAs, but also for the supervisory authorities that have to respond within the timeframes stipulated in the GDPR.

It is important to note that failure to comply with the GDPR's requirements in respect of DPIAs, including failing to carry out a DPIA, carrying out a DPIA incorrectly or failing to consult the supervisory authority where required, can each result in administrative fines being imposed. The level of fines that can be imposed are up to €10million, or up to 2% of worldwide annual turnover of the preceding financial year, whichever is higher.

How do you actually conduct a DPIA?

It is all good and well understanding that there is a now a requirement to conduct DPIAs, but how do you actually go about this in practice? In addition to the guidance and codes of practice issued by local data protection authorities, the Article 29 Working Party's Guidelines confirm that the GDPR provides a common criteria for DPIAs as listed above, but that there are many possible methodologies. The GDPR allows for flexibility when determining the structure and form of DPIAs. This in turn allows for data controllers to create a DPIA process which best fits within their organisation's working practices, provided that they ultimately 'provide a genuine assessment of risks, allowing controllers to take measures to address them'.

Nevertheless, the Article 29 Working Party does encourage the development of sector-specific DPIA frameworks, enabling specific sector knowledge to be utilised to address the particulars of a certain type of processing operation. Under Annex 2 of the Guidelines, the Working Party has provided a DPIA checklist to ensure the basic requirements of the GDPR are followed, but still allows for different forms of execution. This delves into deeper detail of the 4 criteria listed in Recital 90 of the GDPR.

The Working Party also recommends that an organisation's DPIA framework should involve the appropriate interested parties with defined responsibilities, ensuring a collaborative and well-rounded process. This may include the DPO, data subjects or their representatives, business members, third party processors or an Information Security Officer, to name a few.

When conducting the DPIA, data controllers must also, where appropriate, 'seek the views of data subjects or their representatives'. The Article 29 Working Party considers that those views could be sought through a variety of means, depending on the context. For example, they could be gathered through 'an internal or external study related to the purpose and means of the processing operation, a formal question to the staff representatives or trade/labour unions'.

Conclusions

The Guidelines confirm that there is flexibility in DPIA methodologies, but that organisations should apply the Working Party's checklist when considering what type of DPIA is best for them. The DPIA process should be embedded within an organisation's internal processes and culture, aiding its existing business development, IT security, risk and operational review processes.

The key takeaway is that an Article 35 DPIA is not always required. However, risk assessments of personal data processing activities — the type envisaged by Article 24 — are, and they are intrinsic to an organisation demonstrating its accountability under the GDPR. In order to meet accountability requirements, a DPIA must deliver meaningful and measurable data protection change and risk reduction/management. This can be achieved by implementing appropriate technical and organisational measures to mitigate the identified risks.

Samantha Sayers and Kayleigh Clark
PricewaterhouseCoopers
samantha.sayers@pwc.com
clark.kayleigh@pwc.com