Conducting a General Data Protection Regulation compliant Data Protection Impact Assessment

Philip Nolan
Mason Hayes & Curran

CONDUCTING A GENERAL DATA PROTECTION REGULATION COMPLIANT DATA PROTECTION IMPACT ASSESSMENT

Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) comes into force on 25th May 2018 and marks a significant change in the EU data protection regime. The General Data Protection Regulation will repeal and replace the current Directive 95/46/EC on data protection (Data Protection Directive), which forms the basis for the existing data protection regime. While the General Data Protection Regulation builds on familiar concepts and rules, its scope is far reaching and, in many respects, it extends considerably further than the Directive. In addition to its wider scope, standards have been raised and sanctions are higher. One significant practical introduction is the new requirement to conduct data protection impact assessments (DIPIAs) contained in Article 35 of the Regulation. The Regulation will require controllers to carry out DIPIAs in cases of potentially high-risk processing activities. Controllers will also be required to consult supervisory authorities, commonly known as data protection authorities (DPAs), in certain situations.

DIPIAs are assessments of the impact of anticipated processing operations on the protection of personal data. DIPIAs are designed to measure and demonstrate compliance with the Regulation. This is done by:

- Evaluating processing practices.
- Assessing the necessity and proportionality of processing.
- Managing risks to data subjects.

The penalties for not complying and not properly fulfilling DIPIA requirements attract the lower tier of sanctions under the Regulation. While in the lower tier, they still remain severe. Violations can result in administrative fines of up to EUR10 million or up to 2% of the organisation's total worldwide annual turnover for the preceding financial year.

A positive side-effect of the introduction of DIPIAs will be the abolition of the general obligation to notify data processing operations to DPAs. Rather than generally requiring the notification of data processing operations to DPAs, as is currently required in most EU countries, the Regulation relies on data controllers to assess the impact of envisaged data processing operations and only consult with DPAs on high-risk processing operations.

DIPIAs are not entirely new. While the Data Protection Directive did not require DIPIAs to be carried out, the practice had emerged in a number of member states. The Article 29 Working Party (A29WP) has adopted draft guidelines on DIPIAs which will be of considerable assistance to organisations in ensuring DIPIAs are conducted in a manner which is compliant with the Regulation. The A29WP is clearly of the view that DIPIAs are an accountability tool, to be used to incorporate increased protection for personal data within product and service design processes.

Organisations should consider the following questions, as suggested by A29WP, in order to ensure DIPIAs are compliant with the Regulation:

- When should a DIPIA be undertaken?
- When is a DIPIA not required?
- What about pre-existing processing operations?
- How often should a DIPIA be conducted?
- How should a DIPIA be conducted?
- Who should be consulted for the purposes of conducting a DIPIA?
- What is the prior consultation procedure?
- What form should a DIPIA take?
- What are the consequences of failing to conduct a mandated DIPIA?

WHEN A DIPIA SHOULD BE CONDUCTED

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

Under the General Data Protection Regulation, controllers will be required to undertake DIPIAs before data processing. DIPIAs are essential in instances where the envisaged processing is likely to represent a high risk to the rights and freedoms of individuals (Article 35, General Data Protection Regulation). These can include situations where new technologies are employed in data processing. The Regulation does not define “high risk”. However, it provides the following non-exhaustive list of cases in which DIPIAs must be carried out (Article 35(3), General Data Protection Regulation):

- 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.
In addition, the Regulation indicates that DPIAs must be undertaken (Recital 91, General Data Protection Regulation):

- In case of large-scale processing operations that aim at processing considerable amounts of data and could affect a large number of individuals;
- As required by DPAs, which must publish lists of processing operations that 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
  - are carried out systematically on a large scale.

As DPAs must compile a list of processing operations that require a DPIA (Article 35(4), General Data Protection Regulation), there is likely to be guidance from local DPAs in the coming months.

For processing operations other than those specified above, the A29WP lists ten criteria that must be considered when determining whether a processing operation requires a DPIA. Bearing in mind these guidelines, organisations should ask the following questions to ascertain whether it is necessary to conduct a DPIA:

- Are you undertaking evaluation or scoring, including profiling and predicting, of aspects specific to the data subject, such as credit monitoring and genetic testing?
- Does the processing involve automated decision making that produces a significant effect on the data subject?
- Are you performing systematic monitoring of data subjects, including in a publicly accessible area?
- Does the processing involve sensitive data (as defined in Article 9 of the Regulation) or data regarding criminal offences?
- Is the data being processed on a large scale? As there is no definition of large scale processing in the Regulation, (although recital 91 is of some assistance) the A29WP recommends the following factors be given particular consideration in ascertaining whether the processing is being carried out on a large scale:
  - the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
  - the volume of data and/or the range of different data items being processed;
  - the duration, or permanence, of the data processing activity; and
  - the geographical extent of the processing activity.
- Have datasets been matched or combined?
- Does the data concern vulnerable data subjects (as defined in Recital 75 of the Regulation)?
- Is this an innovative use or does it apply technological or organisational solutions (for example, combining use of fingerprint and facial recognition)?
- Are you transferring data outside the EU?
- Will the processing itself prevent data subjects from exercising a right or using a service or contract?

The guidelines offer a general rule of thumb that processing operations meeting at least two of these criteria will require a DPIA. However, a processing operation meeting only one criterion may require a DPIA, depending on the circumstances. The A29WP guidelines also recommend using a DPIA when a processing operation is using new data processing technology. If in doubt over whether a DPIA is required, it is prudent to err on the side of caution and carry out a DPIA.

**WHEN A DPIA IS NOT REQUIRED**

The A29WP has explained that a DPIA is not required in the four specific cases:

- Where the processing is unlikely to lead to a high risk to the rights and freedoms of the underlying data subjects (Article 35(1), General Data Protection Regulation).
- When the nature, scope, context and purposes of the processing are very similar to existing processing activities for which a DPIA has already been carried out. If the new activity is very similar to an existing processing operation for which a DPIA has been carried out, the results of the earlier DPIA can be used (Article 35(10), General Data Protection Regulation).
- Where a processing operation has a legal basis in EU or member state law, and that legal basis states that an initial DPIA does not have to be carried out. The legal basis must regulate the specific processing operation and a General Data Protection Regulation-compliant DPIA must have already been carried out as part of the establishment of that legal basis (Article 35(10), General Data Protection Regulation).
- Where the processing is included on a list established by the DPA of processing operations for which no DPIA is required (Article 35(5), General Data Protection Regulation).

**PRE-EXISTING PROCESSING OPERATIONS**

The General Data Protection Regulation 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 Regulation provisions start to apply. Similarly, once a DPIA has been carried out, the question arises if it must ever be revisited or repeated during the lifetime of the processing operation.

On the one hand, it is burdensome to expect organisations to assess all of their existing processing operations to determine whether they need to be subjected to a DPIA under the Regulation, and then to carry out any necessary DPIAs. A need to repeatedly engage in DPIAs for the same processing activity would also be very onerous. On the other hand, turning a blind eye to existing processing operations, or choosing to run a DPIA once and then never to revisit its content, runs the risk that data subjects' interests could be overlooked.

The A29WP has strongly recommended that a DPIA should be carried out for any data processing operations that are already underway and would meet the test requiring a DPIA, even before May 2018.

In relation to repeating or reviewing DPIAs, Article 35(11) of the Regulation requires controllers to carry out reviews to assess if processing is carried out in accordance with the DPIA “at least when there is a change of … risk”. In addition, the A29WP recommends that as a matter of good practice, DPIAs should be continuously carried out, and re-assessed after three years, and in certain cases more frequently.

**HOW OFTEN A DPIA SHOULD BE CONDUCTED**

Using DPIAs as a mechanism for building privacy concerns into an organisation’s product and service design processes requires organisations to carry out the DPIAs before the processing begins (Articles 35(1) and 35(10), Recitals 90 and 93, General Data Protection Regulation). The A29WP recommend a DPIA should therefore be commenced “as early as practical”, even where aspects of the processing operation remain unknown. The consequence of commencing a DPIA in advance of the processing may mean that DPIAs will frequently require review once processing has started. However, the A29WP points out that this is no excuse for postponing or failing to engage in a DPIA.

Viewing DPIAs as an accountability tool and bearing in mind the changing nature of risks, it is prudent to conduct DPIAs on an ongoing basis throughout the duration of the lifecycle of a processing operation. As noted above, the A29WP recommends
that a DPIA should be re-assessed after three years at the very least.

WHO SHOULD BE CONSULTED WHEN CONDUCTING A DPIA

Ultimately, the controller is responsible for conducting the DPIA, regardless of whether the controller or another entity carries out the DPIA. Although the controller is ultimately responsible for conducting the DPIA, it will be obliged in certain circumstances, or in other cases where it considers it useful, to consult with various parties for the purposes of conducting a DPIA. Those parties may include the:

- Data Protection Officer (DPO). If an organisation has a designated DPO, the General Data Protection Regulation requires the controller to seek the advice of that DPO when carrying out a DPIA (Article 35(2), General Data Protection Regulation).
- Processors. The A29WP suggests that where the processing operation is performed wholly or partly by a data processor, the processor must assist the controller in conducting the DPIA and must provide any necessary information.
- Data subjects. The Regulation specifies that "where appropriate" the controller must seek the views of data subjects or their representatives. However, there is protection for an organisation’s intellectual property and business interests, as this obligation is without prejudice to the protection of commercial or public interests or the security of processing operations (Article 35(9), General Data Protection Regulation).

The A29WP guidance suggests a number of methods could be used to obtain the views of data subjects, depending on the context. These can include a study, a formal question to the staff representatives or trade/labour unions or a survey sent to future customers. The A29WP also emphasises the importance of documenting these consultation processes. Where a data controller’s final decision differs from the views of the data subjects, the A29WP advises that the data controller should document the reasons in support of its decision. Similarly, where a data controller decides that it is not appropriate to seek the views of data subjects, the A29WP recommends that the reasoning for this decision should also be recorded.

- DPA. If the outcome of the DPIA indicates a high risk in the absence of risk mitigation measures, the controller must consult the DPA before commencing processing operations (see below, When and how a DPA should be consulted) (Article 36, General Data Protection Regulation).

Depending on the context of the processing, it may be prudent and helpful to consult with additional parties for the purposes of conducting a DPIA. The A29WP suggests the following additional parties with whom controllers may consult:

- Responsible business units.
- Independent experts of different professions including lawyers, technicians, security experts, sociologists, ethics advisors and so on.
- The Chief Information Security Officer (CISO), if appointed, and/or the IT department.

WHEN AND HOW A DPA SHOULD BE CONSULTED

If a DPIA carried out by a controller indicates that a planned processing would result in a high risk in the absence of risk-mitigating measures by the controller, the controller must consult the DPA before the processing (Article 36, General Data Protection Regulation). Recital 34 of the General Data Protection Regulation appears to slightly soften this requirement by providing that a consultation might not be required if the controller believes that the identified risk can be mitigated by reasonable means in terms of available technologies and costs of implementation. This underscores the importance of considering privacy safeguards and risk mitigation from the outset.

As part of the prior consultation process, a controller must furnish the following information to the DPA (Article 36(3), General Data Protection Regulation):

- 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.
- Any other information requested by the DPA.

After consultation, and if the DPA considers the intended processing would infringe the Regulation, the DPA has an eight-week period to issue written advice to the controller. The eight-week period can be extended by six weeks in complex matters. The period can also be indefinitely suspended until the DPA has obtained all information requested for the purposes of a consultation. As a result, the consultation process may take considerably longer than the projected eight-week period. In addition, Recital 94 of the Regulation clarifies that a lack of response from a DPA within the defined period will not prevent a DPA from exercising its powers, such as the power to prohibit processing operations. Therefore, a lack of response to a consultation request does not confirm that an envisaged processing is compliant with the Regulation nor does it mean that DPA will not take action against the processing. This may lead to considerable uncertainties in practice.

WHAT FORM A DPIA SHOULD TAKE

The appropriate form of a DPIA will differ to suit each organisation. Entities that routinely process complex and large-scale personal data sets should prepare a DPIA questionnaire for the use of the responsible team, which may include technical teams, human resources, product teams, sales/marketing personnel and legal/compliance personnel.

The General Data Protection Regulation contains some guidance as to the features of a DPIA (Article 35(7), General Data Protection Regulation). The A29WP notes that each of the stages is likely to be revisited multiple times before the DPIA can be completed. The stages envisaged are:

- Describe the proposed processing.
- Assess the necessity and proportionality of the processing operations in relation to the purposes.
- Assess the measures envisaged to demonstrate compliance.
- Assess the risks to the rights and freedoms of data subjects.
- Set out 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 Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned with the envisaged processing.

There is no requirement to publish a DPIA under the Regulation. However, the A29WP recommends that data controllers consider publishing all or part of their DPIA so as to assist in the fostering of trust in the controller’s data processing operations and to assist in the demonstration of both accountability and transparency. The A29WP notes that it is particularly good practice to publish a DPIA where members of the public are affected by the processing.
operation. Where controllers are considering publishing all or part of their DPIA, thought should be given to whether this could result in the disclosure of commercially sensitive information, or inadvertently create security risks for the data controller. A summary of the DPIA’s core findings may be more appropriate in these circumstances.

In Annex 2 to its guidance, the A29WP sets out a useful template which organisations can use to assess whether a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the Regulation.

CONSEQUENCES FOR ORGANISATIONS FAILING TO CONDUCT A MANDATED DPIA

Failure to comply with the DPIA requirements can result in significant fines being imposed by the competent DPA. The following omissions can each result in an administrative fine of up to EUR10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher:

- Failure to carry out a DPIA when the processing is subject to a DPIA.
- Carrying out a DPIA in an incorrect manner.
- Failure to consult the competent DPA where required.

Bearing in mind the significant potential fines for organisations who fail to carry out, or correctly carry out, a DPIA, it is important that data controllers familiarise themselves with Article 35 of the General Data Protection Regulation.

At the outset, in determining whether or not a DPIA is required, it is important to establish whether or not the proposed processing operations are likely to result in a high risk to the rights and freedoms of natural persons. Outside the circumstances specifically listed in Article 35, the A29WP’s ten criteria will be of considerable assistance to organisations in this respect. Once it is established that a high risk is likely, organisations must turn their focus to the content of the DPIA and the frequency with which the DPIA should be conducted while bearing in mind the specific nature of the processing operation. Accordingly, entities that routinely process complex and large-scale personal data sets are advised to prepare a template DPIA for future use, and to familiarise responsible personnel with the completion of that template.
Practical Law Contributor profile

Philip Nolan, Partner, Head of Commercial
Mason Hayes & Curran
T +353 1 614 5078
F +353 1 614 5001
E p Nolan@mhc.ie
W www.mhc.ie

Professional qualifications. University of Oxford (BCL (Oxon)); University College Dublin (BCL, Int Law); DePaul College of Law, Chicago (BCL Int); Solicitor, Ireland.

Areas of practice. Privacy and data security; technology law; commercial contracts

Recent activity

- Detailed GDPR compliance planning with a number of the world’s leading technology companies.
- Facebook’s standing EU privacy counsel, and assisted Facebook throughout its audits by the Irish privacy regulator. Oversee the firm’s engagement with Facebook, which includes significant litigation and law enforcement work.
- Advising Twitter in relation to privacy compliance and overseeing the Mason Hayes & Curran internet litigation team that successfully represented Twitter in a number of take down cases.
- Lead the Mason Hayes & Curran team which assisted LinkedIn through its audit by the Irish privacy regulator and advising LinkedIn in relation to pan-EU privacy compliance.

Languages. English

Professional associations/memberships.

- Member and regular speaker at International Technology Law Association.
- Member of AIJA and former President of AIJA’s Technology, Media and Intellectual Property Commission.
- Previous Member, Editorial Board of the Gazette of the Law Society of Ireland.

Publications.

- Irish Information Technology Law, Cavendish.
- Business Law, Oxford University Press.