WILMERHALE

Data Protection Impact Assessments under GDPR: Article 29 Working Party Adopts Draft Guidelines

APRIL 14, 2017

The EU General Data Protection Regulation's (GDPR) requirements are coming into focus quickly as EU data protection authorities continue to issue guidance on different aspects of the law. On April 4, 2017, the Article 29 Working Party (Working Party) continued this trend by adopting draft Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (Guidelines). The Working Party is asking for comments regarding this draft document by May 23, 2017. The document will then likely be finalized at one of the upcoming plenary meetings of the Working Party.

The Guidelines are the Working Party's first step in seeking to promote common criteria, methodology, and recommendations with respect to DPIAs under the GDPR. Companies should take note, and they should begin to consider how they will integrate DPIAs into their day-to-day operations. As with other aspects of the GDPR, non-compliance with DPIA requirements can result in fines of up to 2% of the respective group of companies' global revenue from the preceding year.

What is a DPIA?

The GDPR does not formally define the concept of a DPIA. However, Article 35(7) sets out the minimum content of a DPIA, and Recital 84 of the GDPR clarifies the meaning and role of a DPIA as follows: "*In order to enhance compliance with this Regulation* ***where processing operations are likely to result in a high risk to the rights and freedoms of natural*** *persons, the controller should be responsible for the carrying-out of a data protection impact assessment to* ***evaluate, in particular, the origin, nature, particularity and severity of that risk***." (Emphasis added).

A DPIA may concern a single data processing operation. However, the Guidelines clarify that it also may cover a *set* of similar processing operations, for example, where a group of data controllers are engaged in similar data processing operations or when the same technology product is likely to be implemented by several different data controllers. In such cases, the Guidelines note that each data controller is responsible for carrying out its own DPIA, but that data controllers and/or technology providers may coordinate with each other in carrying out their DPIAs or, in the case of joint controllers, in defining their respective obligations.

When is a DPIA mandatory under the GDPR?

Under Article 35(1) of the GDPR, a DPIA is required when the processing is "***likely to result in a high risk to the rights and freedoms of natural persons***." (Emphasis added). Article 35(3) provides several examples of such circumstances, but the Guidelines set out more specific criteria that should be considered. Specifically, a DPIA may be required if the processing operations involve:

- **Evaluation or scoring, including profiling and predicting**: especially from "aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (Recitals 71 and 91);
- **Automated-decision making with legal or similar significant effect** (Article 35(3)(a));
- **Systematic monitoring** (Article 35(3)(c));
- **Sensitive data**: this includes "special categories of personal data" (sensitive data) as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences;
- **Data processed on a large scale**: the GDPR does not define what constitutes "large-scale," but Recital 91 provides some guidance and the Working Party recommends that the following factors be considered:
  - 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.
- **Data sets that have been matched or combined**;
- **Data concerning vulnerable data subjects** (Recital 75);
- **Innovative use or applying technological or organizational solutions**;
- **Data transfer across borders outside the European Union** (Recital 116); and
- **When the processing in itself "prevents data subjects from exercising a right or using a service or a contract"** (Article 22 and Recital 91).

The Guidelines clarify that, as a rule of thumb, data processing operations that meet at least two of these criteria will require a DPIA. But, in the view of the Working Party, even a processing operation that meets only one of these criteria may require a DPIA in certain circumstances.

The Guidelines also clarify that a DPIA is not required in certain circumstances, such as when the nature, scope, context, and purposes of the processing are very similar to the processing for which a DPIA has already been carried out.

What about already existing processing operations?

The Guidelines note that the requirement to carry out a DPIA applies to processing operations initiated ***after*** the GPDR becomes applicable on May 25, 2018. However, the Working Party "strongly recommends" carrying out a DPIA for processing operations that are already underway, and a DPIA may be required for existing processing operations where:

- A significant change to a processing operation takes place after May 2018, for example because a company uses a new technology or uses personal data for a different purpose;
- Risks change as a result of changes to one of the components of the processing operation (data, supporting assets, risk sources, potential impacts, threats, etc.) or because the context of the processing evolves (purpose, functionalities, etc.); or
- The organizational or societal context for the processing activity has changed.

The Guidelines also recommend that DPIAs be continuously carried out or reassessed after 3 years, or perhaps sooner if necessary.

How do companies implement a DPIA?

The Guidelines emphasize that a DPIA should be carried out ***prior to the processing***. The Working Party recommends taking a "privacy by design" approach (*e.g.*, starting early and updating the DPIA throughout the lifecycle of the project) and treating the DPIA as a "continual process, not a one-time exercise." The Guidelines also discuss in detail what features are required when conducting a DPIA, and offer the following key recommendations:

- **Choose a DPIA methodology** (examples are given in Annex 1 of the Guidelines) that satisfies the criteria in Annex 2 of the Guidelines (which provides a helpful checklist to assess whether a DPIA is sufficiently comprehensive to comply with the GDPR), or specify and implement a systematic DPIA process that:
  - Is compliant with the criteria in Annex 2 of the Guidelines;
  - Is integrated into existing design, development, change, risk and operational review processes in accordance with internal processes, context and culture; and
  - Involves the appropriate interested parties and define their responsibilities clearly (controller, DPO, data subjects or their representatives, business, technical services, processors, information security officer, etc.).
- **Provide the DPIA report to the competent supervisory authority when required to do so**;
- **Consult the supervisory authority when the data controller has failed to determine sufficient measures to mitigate the high risks**;
- **Periodically review the DPIA** and the processing it assesses, at least when there is a change of the risk posed by processing the operation; and
- **Document the decisions taken**.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207