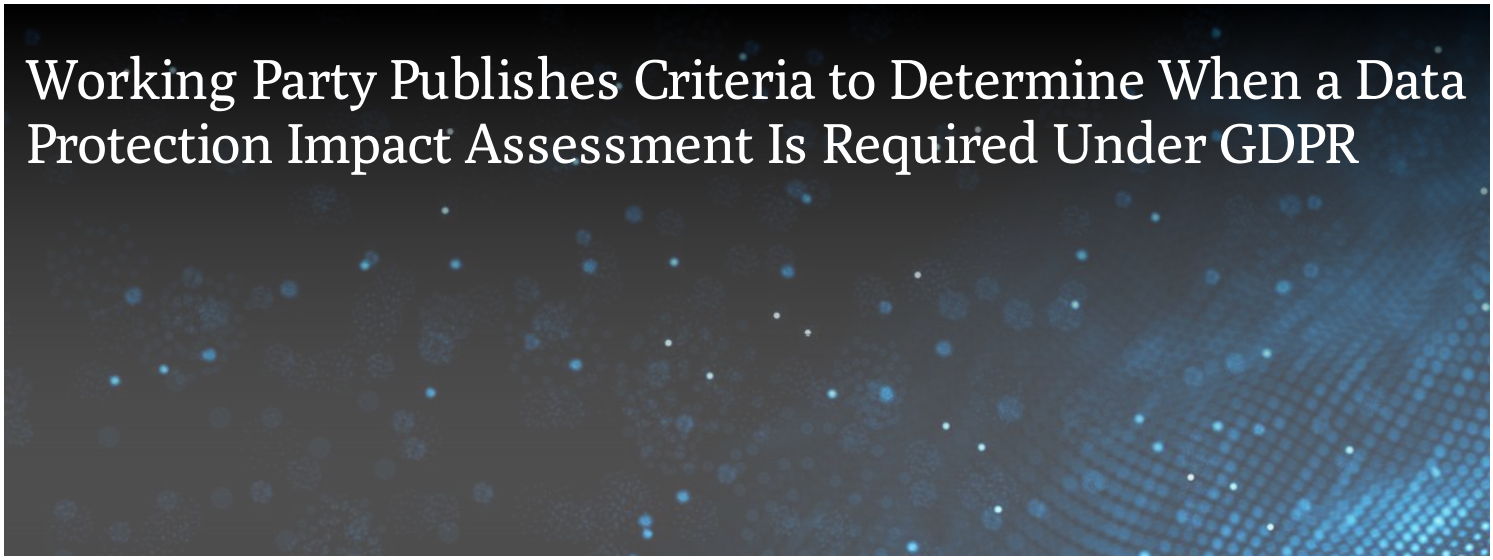
WINSTON & STRAWN LLP

BLOG

Working Party Publishes Criteria to Determine When a Data Protection Impact Assessment Is Required Under GDPR



NOVEMBER 17, 2017

The EU Data Protection Working Party (Working Party) recently published guidelines (Guidelines) regarding when a company operating in the EU must conduct a Data Protection Impact Assessment (DPIA) under the EU General Data Protection Regulation (GDPR) that becomes effective May 2018. A DPIA is a process designed to help companies build and demonstrate compliance with GDPR. A DPIA is required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons." The Working Party set forth criteria to provide a more concrete set of processing operations that require a DPIA due to their inherent risk. Those criteria are:

1. **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" (e.g., a financial institution that screens its customers against a credit reference database);
2. **Automated decision making with legal or similar significant effect**, namely, processing that aims at taking decisions on data subjects producing "legal effects concerning the natural person" or which "similarly significantly affects the natural person" (e.g., processing that may lead to the exclusion or discrimination against individuals);
3. **Systematic monitoring**, such as processing used to observe, monitor, or control data subjects, including data collected through networks or "a systematic monitoring of a publicly accessible area";
4. **Sensitive data or data of a highly personal nature** (e.g., a general hospital keeping patients' medical records);
5. **Data processed on a large scale**;
6. **Matching or combining data offsets** (e.g., originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject);
7. **Data concerning vulnerable data subjects** (e.g., children or employees);
8. **Innovative use or applying new technological or organizational solutions** (e.g., combining use of fingerprint and face recognition for improved physical access control); and
9. When processing in itself "**prevents data subjects from exercising a right or using a service or a contract**" (e.g., where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan).

In most cases, a data controller can consider that a processing meeting two criteria would require a DPIA to be carried out. In general, the more criteria that are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA, regardless of the measures which the controller plans to adopt.

TIP: Companies should analyze these criteria to determine whether they should conduct a DPIA in connection with GDPR compliance.

2 Min Read

Author

Mary Katherine Kulback

Related Locations

Chicago

Related Topics

Europe Privacy

Data Breach

Related Capabilities

Privacy & Data Security

Related Regions

Europe

Related Professionals

Mary Katherine Kulback

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.