
The EU's Article 29 Working Party Releases Guidelines Ahead of GDPR Implementation and Addresses the Privacy Shield

DECEMBER 19, 2016

The EU's Article 29 Working Party (WP29) held a plenary meeting in early December 2016. At the meeting, the WP29 adopted guidelines and issued FAQs relating to the EU General Data Protection Regulation's (GDPR's) provisions on (1) the right to data portability, (2) data protection officers (DPOs), and (3) lead supervisory authorities (LSAs). These long-awaited guidelines are designed to clarify how the GDPR will change the rights and responsibilities of data controllers, data processors, and data subjects. The WP29 also addressed the US-EU Privacy Shield. We've summarized the highlights below.

The guidelines are not final yet; stakeholders may comment on these guidelines through the end of January 2017. For more information and to review the full guidelines and FAQs, please visit ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Data Portability

Article 20(1) of the GDPR provides that in certain circumstances, a "data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format." The article also gives data subject the right to have a data controller transmit that data directly to another data controller.

The new guidelines clarify that, in the view of the WP29, data "concerning" the data subject includes pseudonymous data that can be linked to a data subject and may even include data about third parties. Further, data "provided" by the data subject is broadly construed: it includes data "actively and knowingly provided" by the subject but also "observed" data, such as location data or search history. The only types of data *not* considered to be "provided" by a subject are "inferred" or "derived" data such as algorithmic results (although a data subject may still have the right to access these data).

The guidelines explain that that when a data subject transmits his/her personal data to a new controller, and those data include information about third parties, the new controller cannot use the third-party data for its own purposes. The guidelines also clarify that controllers must explain to data subjects the right to data portability, help them understand what data can be provided, and provide

data in a format that supports re-use.

Data Protection Officers

DPOs are responsible for helping to ensure compliance with data protection laws, but the guidelines make clear that the data controller or processor, not the DPO, bears the ultimate responsibility for compliance. While the use of DPOs predates the GDPR, Article 37(1) of the GDPR requires a private data controller or processor to appoint a DPO where, “the core activities of the controller or processor” either “require regular and systematic monitoring of data subjects on a large scale” or “consist of processing on a large scale of special categories of data ... and personal data relating to criminal convictions and offences...”

The guidelines clarify that “core activities” include activities “where the processing of data forms an inextricable part of the controller’s or processor’s activity.” Whether processing occurs on a “large scale” turns on the number of data subjects or their proportion relative to the population; the volume or range of data involved; and the duration or geographical extent of the processing. The WP29 notes that a more objective understanding of “large scale” may develop over time. Organizations that aren’t required to appoint a DPO can voluntarily do so, but even these DPOs are governed by the terms of the GDPR. The WP29 recommends that controllers and processors that determine they don’t need a DPO document the reasons for that determination unless the determination is obvious.

Article 38(1) requires that the DPO be involved “in all issues which relate to the protection of personal data.” The guidelines explain that they should become involved with these issues at the earliest possible time, are informed, participate in meetings with management, and are quickly consulted when a data security incident occurs. Further, if an organization declines to listen to a DPO’s advice, it should document its reasons for doing so. Article 38(2) requires that DPOs be given sufficient resources. The guidelines clarify that DPOs must be given sufficient time, money, staff, infrastructure, training, and access to other parts of the organization. The guidelines also clarify how organizations can maintain the independence and integrity of DPOs, as required by the remaining provisions of Article 38.

Lead Supervisory Authorities

Article 51 of the GDPR requires each Member State to establish at least one supervisory authority to oversee compliance with the Regulation. The GDPR provides a “one stop shop” mechanism so that organizations engaged in cross-border processing can deal primarily with one supervisory authority—the LSA—instead of multiple supervisory authorities.

Article 4(23) of the GDPR defines cross-border processing as the “processing of personal data” either (1) in a controller’s or processor’s “establishments” in more than one EU Member State, or (2) which “substantially affects or is likely to substantially affect data subjects in more than one Member State.” Whether processing “substantially affects” a subject is determined on a case-by-case basis, turning on, among other things, the risk of “damage, loss, or distress” to individuals; the effect on the individual’s well-being or financial status; and the extent of data processed.

Where a controller or processor has establishments in more than one Member State, the supervisory authority in the jurisdiction of the organization's main establishment is the LSA. The main establishment is "the place where decisions about the purposes and means of the processing of personal data are taken." Often, this will be a controller's central administration, or headquarters. But if a controller has multiple establishments, the main establishment will be the one that makes decisions about a specific processing activity. The guidelines include a non-exhaustive list of factors for determining which establishment is the main establishment for purposes of identifying the LSA.

US-EU Privacy Shield

At the plenary meeting, the WP29 also addressed the US-EU Privacy Shield. First, it adopted "specific communication tools" for individuals and companies, which will be posted online and which national data protection authorities can also use. Second, officials from the United States Department of Commerce, FTC, and the Office of Director of National Intelligence discussed collaboration with the WP29. Third, the WP29 clarified that it will serve as the centralized body handling complaints under the Privacy Shield. The WP29 will finalize more measures at its next plenary meeting in February 2017.

Authors



**Dr. Martin
Braun**

PARTNER

✉ martin.braun@wilmerhale.com

☎ +49 69 27 10 78 207