SQUIRE PATTON BOGGS

WP29 Offers Guidance on DPOs, Data Portability and Lead Supervisory Authority

On December 16, 2016, the Article 29 Data Protection Working Party (WP29) published the much anticipated Guidelines, together with FAQs, providing more guidance on three important concepts under the General Data Protection Regulation (GDPR): (1) Data Protection Officers (WP 243); (2) the right to data portability (WP 242); and (3) the identification of the lead supervisory authority (WP244). The published guidelines are based on input from various stakeholders, including the workshop (Fablab) that the WP29 organized in July 2016 (a summary of the discussions at the Fablab are available online). Stakeholders have until the end of January 2017 to comment on the guidelines.

Data Protection Officers (DPOs)

Under Article 37 of the GDPR, companies are required to appoint a DPO where: (a) the company is a public authority processing personal data; (b) the "core activities" of an entity involve "regular and systematic monitoring of data subjects on a large scale;" or (c) the "core activities" of an entity involve "large scale" processing of "special categories of data" (e.g., health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, sex life or sexual orientation) or personal data relating to criminal convictions and offences. In the WP29's new guidance and FAQs, the WP29 discusses and clarifies when a DPO must be appointed and the duties of the DPO.

WP29 Encourages All Organizations to Have a DPO

The guidelines provide insight on what is meant by the terms "core activities," "large scale" and "regular and systematic monitoring" so that organizations have a better understanding of when they are required to appoint a DPO.

- **Core Activities:** Recital 97 of the GDPR clarifies that "core activities" relate to "primary activities and do not relate to the processing of personal data as ancillary activities." The WP29 cautions that "core activities" can include activities where the processing of data forms an inextricable part of the controller's or processor's activities, and identifies a hospital's processing of health records to provide healthcare as an example. The WP29 specifically notes, however, that an organization's payroll or IT activities are necessary to support a business and therefore are ancillary rather than the core activities.
- **Large Scale:** While Recital 91 of the GDPR provides some guidance, the GDPR does not define what constitutes "large scale." In the guidelines, the WP29 states that "large scale" must be determined on a case-by-case basis, taking into account several factors including: the number of data subjects concerned, the volume of data, and the duration and geographic extent of processing. Some of the examples of large scale processing cited are: processing of personal data for behavioral advertising by a search engine; processing of the real-time geolocation data of customers of an international fast food chain for statistical purposes by a processor specialized in providing these services; and processing of customer data in the regular course of business by an insurance company or a bank. An example that does not constitute large-scale processing is the processing of patient data by an individual physician.
- **Regular and Systematic Monitoring:** Recital 24 of the GDPR makes clear that "monitoring the behavior of data subjects" includes tracking and profiling on the internet. After analyzing what is meant by the terms "regular" and "systematic" in the guidelines, the WP29 advises that "regular and systematic monitoring" includes all forms of ongoing, recurring or periodic, organized or systematic tracking and profiling. Some of the examples listed in the guidelines include providing telecommunications services; email retargeting; profiling and scoring for purposes of risk assessment (e.g., credit scoring, fraud prevention); behavioral advertising; monitoring wellness, fitness and health data via wearable devices; connected devices.

Irrespective of any legal obligation, the WP29 encourages organizations to designate a DPO on a voluntary basis. The same GDPR DPO requirements will apply to such voluntary DPOs.

A Single, Skilled, Autonomous DPO Involved in All Data Protection Issues

The guidelines note that an organization can designate a single DPO as long as that individual is "easily accessible for each establishment." The DPO must be in a position to efficiently communicate with data subjects and cooperate with supervisory authorities, meaning that the communication must take place in the language used by those parties. The WP29 stresses the importance of the DPO being involved in all issues relating to the protection of personal data, necessary resources and the DPO's independence.

The WP29 clearly distinguishes between the role of the data controller or processor, which is responsible for compliance with the GDPR, and the DPO, who, among other things, should assist the controller or processor to monitor internal compliance with the GDPR and has a duty to provide advice as regards data protection impact assessments. The guidelines stress the importance of the DPO being involved in all data protection issues at the earliest stage possible, and of DPOs being provided with the necessary resources and support to fulfill their duties.

The WP29 defines certain minimum requirements regarding the expertise and skills of the DPO, which may be an internal (in-house) DPO or an external DPO appointed on the basis of a service contract. The guidelines specifically state that the expertise of the DPO "must be commensurate with the sensitivity, complexity and amount of data an organization processes." Additionally the DPO should have a deep understanding of the GDPR, and have expertise in national and European data protection laws and practices. In relation to employing an external DPO, the WP29 notes that while organizations could have teams of individuals serving as DPOs, for the legal clarity it should assign a single individual as a lead contact. The guidelines discuss the criteria of independence and possible conflict of interests.

Finally, the WP29 recognizes that Article 37 of the GDPR applies to both controllers and processors, but notes that there may be instances where a controller and processor are not both required to designate a DPO. One example provided is where a small family business distributes household appliances in a single town and uses the services of a processor for website analytics services and targeted advertising and marketing. In such a situation the family business does not engage in the processing of data on a large scale, whereas the processor, with many customers like this family business, is carrying out large scale processing. Thus, the processor must designate a DPO, but the family business (controller) does not need to do so.

What This Means for Companies

- ✓ Unless it is obvious that an organization is not required to designate a DPO, controllers and processors should document the internal analysis conducted in determining whether or not to appoint a DPO.
- ✓ Processors must make an independent assessment regarding their need for a DPO, separate from the controller for which they are processing the data.
- ✓ Organizations required to designate DPOs must: (a) make sure all employees understand the importance of involving the DPO in all data protection issues at the earliest stage possible; and (b) provide the DPO with adequate support so the individual can fulfill his or her duties.

Companies not subject to the mandatory DPO designation should consider whether they want to designate a DPO on a voluntary basis. Companies that employ or engage other privacy professionals must ensure that there is no confusion regarding their title, status, position and tasks with that of the voluntary DPO.

Right to Data Portability

Under Article 20 of the GDPR, data subjects have a right to data portability. In the WP29's new guidance and FAQs, the WP29 discusses and clarifies the scope and limitations of this right, and clearly distinguishes it from the right of access and other rights of data subjects under the GDPR.

At the heart of the guidance, the WP29 focuses on two elements which define the right to data portability, namely: (i) the right to *receive* personal data and store it further for personal use on a device; and (ii) the right to *transmit* the data to another controller without hindrance. Controllers should provide data subjects with personal data "in a structured, commonly used and machine-readable format," and the WP29 calls upon stakeholders to work together to develop a common set of interoperable standards.

The WP29 adopts a very broad interpretation of the scope of the right of data portability, suggesting that the right includes data provided "knowingly and actively" by the data subject (e.g., completing an online form), and data generated by their activity (e.g., data generated by a smart meter). This latter category of data includes raw data collected by virtue of the use of the service or the device, but not inferred or derived data generated by the controller, such as data generated by the subsequent analysis of the data subject (e.g., a credit score or assessment). The personal data must actually concern the data subject. In other words, anonymous data is out of scope; however, pseudonymous data is within scope if it can be clearly linked to a data subject.

The right to data portability does not apply where the processing of personal data is *not* based on consent or contract, such as when the data processing is based on the legitimate interests of the data controller or is necessary for the performance of a task carried out in the public interest, or where the data controller must comply with a legal obligation. However, the WP29 considers it good practice to provide data subjects with a right to data portability in such cases anyway.

In addition, the right to data portability may be restricted where it adversely affects the rights and freedoms of others, including as regards the protection of trade secrets or intellectual property. The WP29 warns controllers not to take an overly restrictive interpretation of these restrictions, noting that a potential business risk is not sufficient to refuse to answer the portability request. In some cases data controllers may process information that contains the personal data of multiple data subjects (e.g., e-mails or telephone records). The guidance recommends that controllers provide records in response to data portability requests even if they contain third-party data.

What This Means for Companies

- ✓ Companies should start to consider and put in place the necessary measures to meet the obligations of the data portability right, which can be met by implementing direct download opportunities, direct transmission to another controller, application programming interfaces (APIs), personal data stores and trusted third parties. The WP29 also stresses the importance of clear and comprehensive information and the need to implement an authentication procedure.
- ✓ Companies should implement tools to enable data subjects to select the relevant data and exclude other data subjects' data, consent mechanisms and also evaluate how portable data can be secured.
- ✓ Companies that believe that some or all of their processing activities are not subject to the data portability obligation should document their assessment leading to this conclusion where this is not obvious.

Identifying the Lead Supervisory Authority

The GDPR introduces the "One-Stop-Shop" principle, which will allow for one supervisory authority (SA), the "lead SA," to oversee cross-border processing activities or processing activities involving the citizens of more than one EU country. In the WP29's new guidance and FAQs, the WP29 discusses and clarifies the designation and duties of the lead SA.

Pursuant to Article 4(23) of the GDPR "cross border processing" means either: (a) the processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor where the controller or processor is established in more than one EU Member State; or (b) the processing of personal data that takes place in the context of the activities of a single establishment of a controller or processor in the EU but substantially affects or is likely to substantially affect data subjects in more than one EU Member State. The guidelines explain that SAs will interpret "substantially affects" on a case-by-case basis and list various factors that will be considered, noting that the *likelihood* of substantial effect is sufficient to bring the processing within the cross-border processing category.

The WP29 notes that: "To fully benefit from the one stop shop mechanism with a single lead supervisory authority for all cross-border processing, companies should consider organizing decision-making powers in respect of personal data processing activities in a single location." Thus, the One-Stop-Shop principle applies only to controllers with an establishment in the EU, and the mere presence of a representative in a Member State (which non-EU controllers or processors that are subject to the GDPR must designate) does not trigger the principle. In such situations (i.e., companies without an EU establishment), the controller or processor must deal with the local SA in every Member State in which they are active.

The guidelines explain how to determine the lead or otherwise competent SA in a number of different scenarios, including by way of examples. The main establishment of the controller is the place of the organization's central administration in the EU, which is the place where decisions about the purposes and means of the processing of personal data are made. The guidelines note that where a multinational company decides to have separate decision-making centers in different countries, more than one lead SA can be identified. Recital 36 of the GDPR explains that if a main establishment does not exist, but many establishments exist, then the main establishment will be where the management activities relating to the processing activities occur. In cases involving both a controller and a processor, the controller's lead SA will be the lead SA for the matter.

The WP29 also recognizes that where processing activities are carried out by a group of related companies with headquarters in the EU, the organization with the overall control is considered the main establishment of the group. Typically the parent company would be considered the main establishment because it would be the place of administration, but this can vary depending upon how the company is structured. However, the GDPR does not permit forum shopping – meaning a company cannot designate a main establishment in an EU Member State where personal data processing decisions are not made.

Importantly, the WP29 recognizes that there will be borderline and complex situations in which the determination of the lead SA will be difficult. When the SAs have conflicting views, the European Data Protection Board will need to become involved to resolve the dispute.

What This Means for Companies

- ✓ The controller or processor should establish whether they carry out any cross-border data processing.
- ✓ It is for the controller itself to identify where its main establishment is located, subject to a subsequent challenge by the respective SA; this assessment should be documented.
- ✓ Companies should be aware that there might be more than one lead SA, if they have separate decision-making centers in different EU countries for different processing activities.
- ✓ Companies not established within the EU must deal with the local SA in every Member State in which they are active.
- ✓ Where an issue arises that involves both a controller and its processor, the controller's lead SA will oversee the issue.

What is Next?

The WP29 will be publishing guidelines on Data Protection Impact Assessments and Certification in 2017. It is also planning a new Fablab in April 2017 for an exchange with stakeholders, and will host a meeting in May 2017 with its international counterparts. We expect that these events will provide companies with further guidance on GDPR compliance issues, as many grey areas remain to be clarified.

Contacts

Annette Demmel
Partner, Berlin
T +49 30 7261 68 108
E annette.demmel@squirepb.com

Monika Kuschewsky
Partner, Brussels
T +322 627 11 11
E monika.kuschewsky@squirepb.com

Ann J. LaFrance
Partner, London
T +44 20 7655 1752
E ann.lafrance@squirepb.com

Gretchen Ramos
Partner, San Francisco
T +1 415 743 2576
E gretchen.ramos@squirepb.com