Recommendations on the Implementation of the General Data Protection Regulation

The European Data Coalition (Coalition) is committed to contribute to the development of a progressive data protection framework, where both clarity and consistency are ensured. In the context of the implementation of the General Data Protection Regulation (GDPR), the Coalition welcomes the ongoing culture of proactive and high-level engagement between all stakeholders including industry representatives, privacy professionals, the European Commission, the European Data Protection Supervisor (EDPS), the Article 29 Working Party (A29WP) and the EU Data Protection Authorities (DPAs).

In December 2016, the A29WP released guidelines on data portability, the role of the data protection officer (DPO) and the one-stop-shop mechanism. While the principles of these 3 concepts are relatively well defined in the GDPR, there is significant margin for interpretation on their scope and application in practice. The Coalition certainly welcomes the shared effort of the European DPAs in clarifying these matters. Following the review of the proposed guidelines, we believe the concerns listed below have not been properly addressed.

Data Portability

Scope

Under the GDPR, the right to data portability has its scope expressly defined: it allows the data subject "*to receive the personal data concerning him or her, which he or she has provided to a controller*". It only applies to personal data an individual has provided to a controller, where the processing is based on the individual's consent or for the performance of a contract, and when processing is carried out by automated means. In addition, the GDPR clearly states that this exercise can only take place "*where technically feasible*".

This right reflects an access right making it possible for data subjects to extract from controllers their own data for personal use. The purpose of this right is, as stressed by the A29WP, to empower the data subject by giving him choice, to encourage innovation in data portability technologies and to introduce competition between data controllers by facilitating the switching between service providers.

While the scope and the spirit of this right is clearly limited under the GDPR, we doubt the necessity and utility of the expansion of its notion in the proposed guidelines to include "*the personal data that are generated by and collected from the activities of users*".

The text of the GDPR limits the scope to what, we believe, should be the data provided directly by the data subject, or, under the wording of A29WG, "*data actively and knowingly provided by the data*

subject". Therefore, **data provided by the data subject by virtue of the use of the service of device – "observed data" – should have been excluded by the A29WG** for the following reasons:

a) This expansion of the scope goes beyond what is required by the GDPR and falls outside the mission of the A29WG, which is to provide expert advice and make recommendations to the public on matters relating to data protection and data privacy in the European Union.
b) In addition, this expansion of the scope is not in line with the objective of the right to portability, because observed data in relation to the data subject are not likely to be similar from one data controller to the next, as they are variable and depend on the processing methods employed by each one. Thus, they do not limit the switching from one service provider to another, nor do they create similar lock-in risks that limit competition and threaten the data subject' right to data protection.
c) An overarching argument derives from the immense and unreasonable costs for data controllers and companies to build an interface that is integrated to all IT systems containing personal data. An excessive interpretation of the scope of this right would also challenge the balance between the data subject's request and the data controller's obligations.

Employment data

The guidelines state that: *"Indeed, the primary aim of data portability is to facilitate switching from one service provider to another, thus enhancing competition between services".* As the portability requirement raises many questions in the employment-context where there is no need to port the data in order to switch service provider, **the guidelines should clearly exclude portability from work-tools provided to the work-force**.

Pseudonymous data

A controller must allow portability not only of data submitted by the data subject (e.g. name, address) but as well data generated by the data subject's use of the controller's services (such as search history, traffic data, or location data). This does not include anonymous data but does include pseudonymous data.

We encourage that pseudonymous data should be excluded from the definition of "*data concerning the data subject*". An obligation to quickly recreate the connection between the data and the data subject is in contrast with the purpose of pseudonymization. Further, it would be very difficult and costly for companies to create such secure solutions. For example, if an online retailer store pseudonymous data to make analysis of general shopping, this information should not be easily recreated to secure the integrity of the customer. The data is important for the retailer to be able to calculate and plan the stock, but it is not used to collect information regarding a specific individual and therefore not of interest for the data subject.

Reconciling data portability with IPRs and trade secrets

The right to data portability could lead to data subjects being able to intrude on trade secrets or other proprietary products the controllers may claim to that data. The proposed guidelines state that "*[t]he right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights. A potential business risk cannot, however, in and of itself, serve as the basis for a refusal to answer the portability request.*"

However, we find lawful for a company to decline a portability request if it believes its trade secrets and *know-how* can be at stake.

Therefore, **the guidelines should go further in specifying under which circumstances a controller can refuse a request for access in order to protect obvious risks to trade secrets**, particularly to:

a) Data concerning the employee which is submitted in the context of an employment task or consulting service should not be used as a profit for the employee/consultant to bring to a competitor.
b) Data related to customer intelligence & analytics, which can cover personal and non-personal data and are derived from customer data that a company lawfully collects from both internal and external sources and by its own developed technical processes, should not be transferred to a competitor, because they have implied specific processes and methods that were designed by the data controller and, as such, should be treated as trade secrets and *know-how*.

Data Protection Officer

Designation of a DPO

Article 37(1) requires the designation of a DPO in three specific cases:

1. *where the processing is carried out by a public authority or body;*
2. *where the core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or*
3. *where the core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences*

The proposed guidelines should provide further clarification on the following definitions:

- Core activities: the A29WP defines "core activities" as "key operations necessary to achieve the controller's or processor's goals." This does not mean that the organization must be in the business of data analytics, however, but rather that data processing is "an inextricable part of the controller's or processor's activity." Would online personal data used in the completion of orders and marketing be considered a core activity?
- Regular and systematic monitoring: with respect to this notion, the examples given in the guidelines are too broad, thereby risking to capture activities that may be regular or systematic but not monitoring. Indeed, some routine systematic processing does not involve the monitoring of individual data subjects. For example, retail companies often have loyalty programs that do not involve monitoring behaviour (e.g. who buys what) but may simply provide bonus points based on the total value or purchased goods. It is important to refine the examples in the guidelines.

Conflict of interest

The Coalition welcomes the A29WP's acknowledgement that determinations of conflict must be casuistic, based on the specificities of the companies and structures involved. Indeed, a case-by-case analysis is crucial in keeping the effectiveness and the full potential a DPO can deliver.

However, some of the examples of conflicts given in the proposed text, including "*roles lower down in the organisational structure if such position or roles lead to the determination of purposes and means of processing*" are problematic. This description is somewhat unclear, to the extent that it disapproves of a "data strategist" function of the DPO and whether it is or not possible for a DPO to also serve as an information security officer (ISO) or chief information officer (CIO).

From our experience, successful DPOs frequently perform the role of chief data strategist. Furthermore, the DPO is in a good position to balance and integrate privacy compliance functions with the strategic use of held personal data. Likewise, we also see no reason to exclude the DPO from exercising other functions such as ISO or CIO, which is particularly valuable for SMEs that often must rely on limited staff to perform several tasks.

Lead Supervisory Authority

Third countries

The guidelines on the functioning of the one-stop-shop and on the definition of the lead Supervisory Authority should give further clarification on the relationship with third countries. For instance, could a customer in a third country file a complaint against a company with the DPA of the Member State where the company has its main establishment?

ABOUT THE COALITION

Our Coalition is made up of twenty European companies, from SMEs to Global Multinationals and non-profit organisations operating in a variety of sectors on a national, regional and global scale. With an aggregate turnover (2015) of over € 222 billion and some 968,000 employees worldwide, our footprint allows us to bring growth, progress and jobs to the EU's economy. Our membership includes…

… a global leader in power and automation solutions…
… a productivity solutions provider of compressors, vacuum solutions, construction and mining equipment…
… a non-profit organisation dedicated to collecting money to prevent and combat child cancer diseases…
… a global leader in household appliances…
… two providers of communications technology and services…
… a designer, engineer, manufacturer and distributor of outdoor power products…
… a multinational retail-clothing company…
… an investment company…
… a SME provider of online marketing through search engine marketing, conversion and lead generation…
… an e-commerce company providing payment services for online storefronts…
… an engineering group in tooling, materials technology, mining and construction …
… an enterprise software corporation…
… a global provider of heavy trucks and buses, engines and services…
… a global provider of renewable solutions in packaging, biomaterials, wood and paper…
… a multinational company managing a portfolio of businesses in retail, financial services and technology…
… the leading university in technology and digital arts programmes…
… a provider of business software and services to more than 340 000 business in the Nordics…
… a producer and distributor of trucks, buses and construction equipment…
… the leading company in advanced mobile services…

Our businesses are profoundly different but deeply united by the need for clear, predictable and practical provisions, open cross-border data flows, balanced codified sanction guidelines, effective one-stop-shop and absence of overly prescriptive rules as fundamental conditions for long-term growth, competitiveness and prosperity, for both us and the economies in which we operate.

For further information please visit us www.europeandatacoalition.eu or contact us at frederico@europeandatacoalition.eu or rene@europeandatacoalition.eu