AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

To: Working Party 29

AmCham EU Comments on the Working Party 29 draft guidelines on portability, DPOs and lead supervisory authority

* * *

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2016, directly supports more than 4.5 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

* * *

American Chamber of Commerce to the European Union (AmCham EU)
Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium
Register ID: 5265780509-97
Tel: +32 (0)2 513 68 92 | www.amchameu.eu

Secretariat Point of Contact: [Maika Föhrenbach]; [mfo@amchameu.eu] +32 (0)2 289 10 11

15 February 2017

Introduction

The American Chamber of Commerce to the European Union (AmCham EU) brings together U.S. companies investing in Europe from a broad range of sectors, including aviation, consumer goods, energy, financial, heavy industry, pharmaceuticals and technology, among others. AmCham EU members typically operate globally with a strong presence in Europe and the Unites States. As such, they may have multiple business units with various governance bodies in more than one jurisdiction, including primary decision-making functions outside of the EU.

With the adoption of the GDPR, the EU recognises the importance of harmonising European data protection laws, in order to facilitate cross-border commerce.

AmCham EU's members take GDPR compliance seriously, and are now working to implement the upcoming rules. In that context, in January 2017, AmCham EU adopted a position paper[1] including recommendations for the data protection authorities (DPAs), the European Data Protection Board (EDPB), and Member States to consider as they develop guidance and policies on the GDPR. The recommendations concern seven specific aspects of the GDPR with the aim of ensuring a uniform and balanced application of them across Europe, i.e.: (i) the one-stop shop; (ii) high-risk processing / data protection impact assessments (DPIAs); (iii) personal data breaches and notification; (iv) approved codes of conduct and certification; (v) data portability; (vi) sanctions; and (vii) data protection officers (DPOs).

When formulating guidance and rules on these and other issues, we encourage regulators to consult regularly and work closely with stakeholders, including industry. In this context, we welcome that the Working Party 29 (hereafter WP 29) decided to submit its draft guidelines on portability, DPOs and identification of the lead supervisory authority to a consultation process with stakeholders. AmCham EU calls the WP 29 to formalise this process even more, notably by providing a timeline for a consultation, and organising open and regular consultations throughout the implementation process. We understand this is in line with the plans announced at the FabLab that took place in July 2016.

Portability

Scope

- AmCham EU welcomes that the WP 29 issued guidance on the new right to "data portability". The data portability concept is novel, and a number of concepts need to be clarified in order for it to work in practice. Data portability should help to enable free flow of data accross the EU. AmCham EU recognizes the importance of this data subject right, however we believe that the WP 29 guidelines need to be more balanced and proportional. The overly broad interpretation of data "provided by" the data subject extends the scope beyond what it is

[1] http://www.amchameu.eu/position-papers/position-paper-amcham-eu%E2%80%98s-recommendations-gdpr-implementation.

needed to guarantee the data portability right and goes beyond the compromise reached in that respect by the EU institutions that adopted the GDPR.

- AmCham EU believes that the interpretation of "provided by the data subject" by the WP 29 is too far-reaching and urges the WP 29 to reconsider it. The right of portability should only cover data actively provided by data subjects. Furthermore where data generated by a data subject's actions on or use of is enriched with any analytics, it should be considered as proprietary to the data controller and thus out of the scope of the data portability right. The WP 29 should clarify that any data which has been enriched with analysis to generate information about a data subject's actions on or use of a service is considered as "inferred data and derived data". At the minimum, the WP 29 should give further guidelines on criteria to frame a portability request and limit the forms of metadata which need to be provided, for instance by defining what forms of metadata can be considered as actively provided by the data subject.
- We also believe that data portability rights would be better understood and implemented by stakeholders in the ecosystem if they were expressly using well-defined and well-understood concepts and terminology. The clarification offered uses nuance descriptions of various types of data and how the data portability rights should be handled based on them and we would recommend that the data portability clarifications are expressed using standardized terminology and concepts where possible.
- In particular, AmCham EU believes that it would be helpful to have clarifications and restrict what data is portable in the employment context (e.g. if an employee is leaving an organisation). Data collected in an employee relationship subject to the right of data portability would in many instances violate current employer's confidentiality interests. AmCham EU's members employ across Europe and would greatly benefit from a common approach to this issue.
- Concerning other data subjects, the WP 29 obliges data controllers (both 'sending' and 'receiving') to implement tools to enable data subjects to select the relevant data and exclude (where relevant) other data subjects' data, as well as to implement consent mechanims for other data subjects involved. AmCham EU questions whether the suggested approach concerning other data subject's data is balanced and offers adequate protection for other data subjects. All the burden is put on the data controller. The Working Party should clarify the criteria for the exercise of the right when other data subject's data are included, such as proportionality, the purpose, feasibility or usability.

Format

- Regarding the excessiveness of a request, we understand that the "overall cost of the processes created to answer data portability requests should not be taken into account to determine the excessiveness of a request". However, we believe that the guidelines are not balanced when stating that "the overall system implementation costs should neither be charged to the data subjects, nor be used to justify a refusal to answer portability requests". In particular for large data controllers, the overall number and nature of requests – which is not the focus of article 12 - could indeed lead to excessive burdens. Therefore, we call the WP 29 to elaborate in its guidelines on criteria or factors for situations that might fit in the definition of "manifestly unfounded or excessive" requests. There is no doubt that such situations might appear.

In this regard, and in line with what has been mentioned above, clarifying the scope and setting clear standards for the application of the scope of the data portability right would help companies comply, and avoid situations of excessive requests.

- In order to enable industry to develop appropriate compliance procedures and capabilities in existing systems, AmCham would have appreciated to have clarifications as to how regulators will interpret the phrase "structured, commonly used and machine-readable". In particular, it would be helpful to clarify that formats using most popular and common standards for structured documents and web data are one option to be compliant, potentially also used in combination with other formats where data cannot be expressed through these common formats.
- Furthermore, we are concerned about the request of the WP 29 to provide as many metadata as possible at the best level of granularity. In general, AmCham EU believes that metadata is often enriched by the data controller and should be considered its proprietary. At the minimum, the WP 29 should give further guidelines on criteria to frame a portability request and limit the forms of metadata which need to be provided.
- Concerning how to deal with large complex personal data collection, WP 29 recommends the use of an Application Programming Interface. AmCham EU calls the WP 29 to clarifiy that this is one option and not a requirement, as it might not be a desirable or suitable option in all sectors of the economy.
- Furthermore, AmCham EU would welcome more guidelines on the notion of technical feasibility and on situations in which it can be considered that the direct transmission of data from one controller to another is not technically feasible. AmCham EU calls the WP 29 to include such clarifications in the draft guidelines and to exclude scenarios where new systems or capabilities would need to be built in order to enable direct exchange.

Data Protection Officers

- AmCham EU welcomes that the Working Party 29 issued guidance on Data Protection Officers (DPOs). Many issues relating to DPOs still lack clarity, in particular the terms "core activity" and "large scale" processing, making it more difficult for our members to be compliant. While the guidelines do not fully clarify these notions, AmCham EU also believes that they are too prescriptive on how a company has to fulfill the obligations of DPO. Our comments aim at better reflecting the diversity of business, corporate structure and resources of companies.

The notion of "core activity"

- In its draft guidance, the WP 29 illustrates the notion of "core activity" with some examples that fall inside or outside of the scope of this notion. AmCham EU welcomes this attempts of clarification but believes that uncertainties remain. AmCham EU understands that normal recruitment or Human Ressources practices do not require a DPO appointment. However, it is unclear for instance to what extent a company's use of cookies to monitor its own websites, or routine use of everyday business contact (e.g. for customer relationship management (CRM), market or contract performance purposes) can be considered as ancillary function or not. AmCham EU calls the WP 29 to clarify that those activities do not require a DPO if they are not part of the core business of a company.
- The WP 29 adopts a narrow interpretation of what data processing as ancillary function of a company is, and a very broad interpretation of what "regular and systematic monitoring" implies. The WP 29 states that the notion of 'monitoring the behaviour of data subjects' "clearly includes all forms of tracking and profilig on the internet".

The notion of "large-scale processing"

- In order to clarify the notion of "large-scale processing" in the draft guidance, the WP 29 recommends a list of factors to be considered and gives some examples. The WP 29 also intends to further contribute to clarifying this notion by publicising examples of the relevant thresholds for the designation of a DPO.
- AmCham EU believes that the WP 29 should closely work with the industry in defining thresholds and best practices.

The role of the DPO

- AmCham EU believes that the guidance given by the WP 29 concerning the liability of the DPO remains too vague. It would be helpful to get more clarity for instance on whether DPOs can be hold accountable to management and boards for its role as DPO. It seems understandable that a DPO cannot be sanctioned for carrying out its mission. However, the WP 29 gives a very conservative view on when a DPO can be dismissed or replaced by another person, which is not consistent with business practice.
- AmCham EU welcomes that the WP 29 clarifies that "the function of DPO can also be exercised on the basis of a service contract concluded with an individual or an organisation outside the controller's/processor's organisation". Furthermore we understand that the role of DPO can also be exercised part-time, and that a DPO might be appointed for serveral bodies. The WP 29 leaves some flexibility on the nature of the person who take the role of DPO.

- However, AmCham EU would like to hear more guidance related to the organisational DPO functions with multiple individuals performing the obligations of a DPO, whether internal or external to the company.
- Furthermore, AmCham EU urges the WP 29 to confirm that a DPO can be physically located outside Europe, while fullfilling the requirement of being 'easily accessible from each establishment'. For instance, if an US-headquartered entities with global operations and presence, including in the EU, makes corporate decisions on processing from the US, if the DPO is to have direct access to these decisions, that would be most effectively accomplished by an individual located in the US.
- On the top of including the additional clarifications listed above, AmCham EU calls the regulators to consult with industry to help produce best practices and working examples.

Lead Supervisory Authority

- AmCham EU welcomes that the WP 29 issued guidelines for identifying a controller or processor's lead supervisory authority. However, the possibility to identify a "main establishment" for all companies whether headquartered or not in the EU, is too restrictive and requires further clarifications.

Identification of the main establishment

- AmCham EU believes that one way to help restore value to the one-stop shop concept, and at the same time to encourage business to invest by boosting business certainty, would be to endorse in guidance the idea that if a company designates a location as its main establishment, for current companies to be done prior to the effective date of the GDPR (May 25, 2018), that designation presumptively decides the issue, unless clearly contrary to facts on the ground or the GDPR. In this regard, AmCham EU regrets that the WP 29 goes beyond the GDPR by assigning the burden of proof to the controllers/processors. A balanced implementation of the GDPR should grant the controller/processor with a rebuttable presumption on the basis of objective facts.
- AmCham EU welcomes the efforts of the WP 29 to clarify the identification of the "main establishment". The WP 29 foresees that in some complex cases, (such as for instance where there is cross-border processing activity and the controller is established in several Member States, but there is no central administration in the EU and none of the EU establishments are taking decisions about the processing), the company would need to designate the establishment that will act as its main establishment. However, the requirement that "this (main) establishment must have the authority to implement decisions about processing activity and to take liability for the processing, including having sufficient assets," is unclear, and makes it questionable how global corporations that are headquartered outside the EU could benefit from a one-stop-shop. AmCham EU urges the WP 29 to clarify such situations as well. The guidance should also address stakeholders' structures that are less pyramidal (e.g. partnerships, franchise networks).

Supervisory Authority Concerned

- AmCham EU welcomes that the WP 29 encourages cooperation between lead and supervisory authorities, and encourages joint controllers to designate a single competent authority to monitor their joint data processing activities.