U.S. CHAMBER OF COMMERCE

U.S. CHAMBER OF COMMERCE COMMENTS ON ARTICLE 29 DATA PROTECTION WORKING PARTY DRAFT GDPR GUIDELINES

JANUARY 2017

The U.S. Chamber of Commerce is the largest business organization in the United States, representing the interests of more than three million businesses of every size, sector, and state, as well as state and local chambers and industry associations. In addition, we represent many European firms with investments and operations in the United States and have been a steadfast supporter of the economic underpinnings of the Atlantic alliance and their benefits for workers, consumers, and companies in both the United States and the EU.

On 13 December 2016, The Article 29 Data Protection Working Party (WP29) released General Data Protection Regulation (GDPR) guidelines on data portability, data protection officers (DPOs,) and identifying a lead supervisory authority as well as the associated Frequently Asked Questions (FAQs). We applaud the WP29's decision to share guidance on GDPR implementation as well as seek comments on the proposed guidance. This helps companies better understand how data protection authorities (DPAs) will interpret and enforce provisions. We welcome the opportunity to comment on these documents.

GENERAL COMMENTS

We welcome the guidelines provided by the WP29, which help provide transparency and clarity to how DPAs expect business to comply with the GDPR. When implementing the GDPR, the WP29 and Member State DPAs must keep in mind the objective of the legislation to harmonize EU data protection laws in order to both better protect and secure individual's data while facilitating cross-border data flows.

Member State DPAs must avoid implementing varying interpretations and enforcement mechanisms; indeed that would defeat the purpose of transitioning data protection from a Directive to a Regulation. Consistency is essential for creating legitimate compliance expectations in the regulatory community.

When enforcing the GDPR, the guidelines should not be interpreted as one-size-fits all standards and examples. Businesses will need to implement the GDPR in a manner that is best for their business model. We believe the best way to ensure successful adoption of the GDPR is to enable this flexibility. Member State DPAs should keep this in mind when enforcing the GDPR.

Continued engagement between regulators and the regulatory community is necessary for the successful implementation of the GDPR. This engagement should not end with the implementation phase, but this opportunity should be used to establish ongoing, structured consultation procedures between the regulatory community and WP29. As the WP29 establishes

its successor, the European Data Protection Board, it should also create an online platform for effective and continued communication with the regulatory community. Member State DPAs should also develop their own consultation procedures that create transparency. The regulatory environment will continue to involve post-GDPR so mechanisms for providing future clarification and consultation must be established now.

Additional Guidance Necessary

We will welcome the opportunity to comment on the two additional sets of the GDPR guidelines on Data Protection Impact Assessments and Certification that the WP29 is scheduled to release in 2017. We also applaud the WP29's new 2017 priority to release guidelines on the topics of consent and profiling and the issue of transparency.

The Chamber encourages further guidance on issues that still need clarity such as legitimate interest, privacy by design, breach notification, and international transfers. We hope that the WP29 will consider adding work on such guidelines to its 2017 Action Plan.

We also encourage further guidance from Member State DPAs similar to efforts by the UK's Information Commissioner's Office (ICO) and Ireland's Office of the Data Protection Commissioner (ODPC). Such guidance will help companies understand what specific DPAs expect for compliance and ensure that companies are able to adequately prepare.

Finally, the WP29 should also provide guidance on how the GDPR will interact with existing and new regulation, particularly the Network and Information Security (NIS) Directive and the recent Commission draft proposal on e-Privacy regulation.

SPECIFIC COMMENTS

Guidelines on the right to data portability

Scope of the Right to Data Portability

The Chamber is encouraged by WP29's limited definition of the right to data portability and the exclusion of data "generated by the data controller". We also welcome that a distinction has been made between the right to portability and the right to access.

However, the WP29 should amend its broad approach by refining the guidance to reflect that the right to portability covers data provided by the subject but not data generated or enhanced by the data controller. In particular, observed data collected from devices and the use of services should be excluded from the portability obligation along with inferred and derived data. Each of these types of data should be considered proprietary as it can be transformed by the data controller or processor; therefore, there is a legitimate interest in protecting the trade secrets and intellectual property created by this data.

The guidance specifically mentions that the right to data portability covers observed data "provided by the data subject" such as "search history, traffic and location data" and "heartbeat tracked by fitness or health trackers". A data controller may add value by further processing such data which includes or results in proprietary information. Under the current interpretation,

this data would not be protected. It may lead controllers to rely on alternative legal basis to process data. The WP29 should not maintain this broad interpretation of the right to data portability to include all observed data.

The guidance further requests data controllers to "provide as many metadata with the data as possible at the best possible level of granularity". This can be interpreted to mean that e-mail data must also include information such as timestamps of when the email was sent and received and whether the email was opened. This level of granularity goes beyond what is in the GDPR. It is likely that this metadata is infused with trade secrets and intellectual property that enables features of value to users. By following this request, businesses may be required to transfer their proprietary information. We suggest that the WP29 acknowledge that metadata can hold trade secrets and intellectual property and should not be subject to the portability obligation.

Data Portability Requests

The WP29 advises that "a form that does not release information covered by trade secrets or intellectual property rights" may be the best method to comply with data portability requests. There may be cases in which the form storing the information on a data subject also holds trade secrets and proprietary information. The actual questions and data points provided in such a form may also be the subject of innovation and trade secrets applied by the controller or processor, thus adding value to the data. Further, sometimes controllers add value to data that is not provided by the data subject but provided by their use of a particular service. More thought and flexibility is needed on how to consider such cases and the best way to handle requests.

The right to portability's intent is to allow data subjects to easily move their data between various services. When moving data, a user may not want to transfer all of the data. The WP29 should allow controllers to simplify this process for users by allowing them options to select which information they want to transfer rather than obliging all data to be transferred. The WP29 should also allow the new receiver of the user's data to decide which information it should process. It is often the case that the receiver may not need to process of the user's data but only the data which serves the purpose of switching services.

The WP29 guidance suggests that data controllers should comply with portability requests in "a very short time-period". It further asks that timeframes for dealing with data portability requests be defined. The Chamber suggests that the WP29 keep in mind the importance of security considerations when determining process timeframes. The guidance should acknowledge the need for security measures. Data portability requests will bring about new security concerns, and protections are necessary for fulfilling data portability requests. Businesses should have the flexibility in their timeframes to authenticate the identity of the data and determine the circumstances in which authentication may be necessary.

The guidance goes beyond what is outlined in the GDPR by advising how data controllers should provide and receive data. The Chamber believes that such decisions should be left to the data controllers as it will vary depending on the service their business provides. Businesses are already leading the way by providing tools to their users that help them select and exclude their data or third party data. By allowing the development of these methods to be market-driven, it better guarantees businesses will be able to utilize the best practices that protect their users and generate competition.

Third Party data

The guidance outlines various requirements and mechanisms for controllers around data portability requests that contain third party data. Controllers must fulfill the request even if third party data is included. The WP29 should clarify the actual legal basis on which the personal data of third parties can be transferred to another data controller without their consent.

Further, the guidance states that the receiving controller must identify its legitimate interest in processing this data. The WP29 should acknowledge that the receiving data controllers need to process the data before they can establish a legal basis or delete the data. Therefore, the guidance should clarify that the legal basis can be assumed to be the data subject's explicit consent unless this can be demonstrated not to be the case.

Data controllers should have the flexibility to offer data subject the ability to manually select that third party data be excluded and verify with the controller that they have done so. In such cases, the data controller should be allowed to rely on the user's verification that third party data is excluded.

The WP29 must avoid placing heavier burdens on the receiving controllers that were not required of the first controller. The guidance outlines that the receiving controller is responsible for ensuring that data not necessary for the purpose of its processing is deleted. This deletion should not be required "as soon as possible" as the guidance outlines, but controllers should be able to follow the storage limitation principle in Article 5(1)(e) of the GDPR.

Data Format

The guidance outlines that the "data must be provided in a structured, commonly used and machine-readable format" and states that the aim is to facilitate interoperability. It further states that "the GDPR does not impose specific recommendations on the format". The Chamber welcomes this clarification but asks that the WP29 acknowledge that the right to data portability does not require controllers to use processing systems compatible with third parties. Further, it should list more examples beyond the API as a possibility to meet the right to portability requirement.

Guidelines on Data Protection Officers (DPOs)

DPO of the Processor

The guidance states that the DPO "should also oversee activities carried out by the processor organization when acting as a data controller in its own right." We believe that the WP29 should clarify that certain processing activities will not require a DPO. In these cases, such as HR processing, the DPO should not be required to be involved.

Conflicts of Interest

The Chamber welcomes the WP29's thinking that conflicts of interest must be determined on a case-by-case basis. We would welcome greater clarification regarding DPO's

functioning as a strategist for their organization. Businesses, especially small businesses, often need their DPO to perform privacy compliance functions and advise on the strategic use of data. We believe these actions can be done without a conflict of interest. We recommend that the WP29 recognize that these functions are in compliance with the functions of a DPO. Industry should be consulted to help produce best practices and working examples to provide further clarity.

Guidelines for identifying a controller or processor's lead supervisory authority

Main Establishment

We appreciate the guidance that advises businesses on how to determine the "main establishment". However, we have reservations about how the guidance outlines its recommendations for borderline and complex situations where it is difficult to determine the main establishment. In particular, we are troubled by the guidance statement that "the burden of proof ultimately falls on controllers and processors." The text of the GDPR does not assign burden of proof in the same manner.

Supervisory authority concerned

We welcome WP29's encouragement of cooperation among lead and supervisory authorities, in particular the goal of reaching mutually acceptable decisions with respect to substantive conclusions; indeed, this is explicitly provided for in Article 60 of the GDPR.

However, the GDPR only provides for limited cooperation with respect to lead and supervisory authorities reaching mutually acceptable decisions on procedural matters. As Article 60(9) outlines, this cooperation is scoped to circumstances "where the lead supervisory authority and the supervisory authorities concerned agree to dismiss or reject parts of a complaint and to act on other parts of that complaint". It does not, as the WP29 suggests, include decisions about issuing a warning or a press statement.

The guidance should make clear that, when in case of doubt, the lead supervisory authority's decision should prevail where it involves making procedural decisions to dismiss or reject part of a complaint.

The Chamber appreciates your consideration of our comments. We would be happy to engage further on any points raised.