AmCham EU's Recommendations on GDPR Implementation

Ensuring a balanced and forward-looking data protection framework in Europe

POSITION PAPER

Executive summary

AmCham EU's recommendations for the implementation of the General Data Protection Regulation (GDPR) address seven specific aspects with the aim of ensuring a consistent and balanced application across Europe:

(i) **The one-stop shop**: To add clarity, where an organisation designates a location as its main establishment, this should presumptively decide how the "main establishment" is determined.

(ii) **High-risk processing and Data Protection Impact Assessments (DPIAs)**: Additional context needs to be provided regarding what constitutes "high risk processing".

(iii) **Personal data breaches and notification**: Guidance is needed regarding the types of breaches that create a "risk" requiring notice to Data Protection Authorities (DPAs), and what additional factors create a "high risk" requiring notice to data subjects.

(iv) **Approved codes of conduct and certification**: They must be pragmatic and should never be less flexible than the basic rules of the GDPR.

(v) **Data portability**: Guidance should clarify that the right covers only data provided by data subjects but not data generated by the service.

(vi) **Sanctions**: A balanced use of full spectrum of powers and dialogue with industry should be endorsed by the European Data Protection Board (EDPB).

(vii) **Data protection officers (DPOs)**: Guidance should clarify, in particular, the meaning of the terms "core activities" and "large-scale processing".

* * *

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 2015, directly supports more than 4.3 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

17 January 2017

AmCham EU – Implementation of the General Data Protection Regulation (GDPR)

The American Chamber of Commerce to the European Union (AmCham EU) brings together U.S. companies invested in Europe from a broad range of sectors, including aviation, consumer goods, energy, financial, heavy industry, pharmaceuticals and technology, among others.

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, AmCham EU has developed the following recommendations for data protection authorities (DPAs), the European Data Protection Board (EDPB), and Member States to consider as they develop guidance and policies on the GDPR.

Our recommendations address seven specific aspects of the GDPR with the aim ensuring a uniform and balanced application across Europe: (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), four of which (DPIAs, codes of conduct/certification, data portability and DPOs) have already been the subject of the first FabLab of July 2016.

General Comment

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 would also like to understand how the WP29 plans to engage with stakeholders throughout the implementation process. This should be a formalised process to allow for all stakeholders to engage their experts and provide expertise. Here a timeline for a consultation would be helpful.

Specific Recommendations (without order of priority)

One-Stop Shop

- The GDPR's one-stop shop mechanism is intended to encourage cross-border data flows and simplify compliance obligations. But there is still a significant lack of certainty as to how the "main establishment" is determined, especially in complex cases. To add clarity, where an organisation designates a location as its main establishment, this should presumptively decide the issue, unless it is clearly contrary to facts on the ground (or the test in the GDPR).

- The urgency procedure, which enables local DPAs to intervene in lead DPA scrutiny, also needs to be carefully circumscribed, in order to prevent conflicts between DPAs and to help preserve the value of the one-stop shop concept. Specifically, the "exceptional circumstances" considered to trigger the urgency procedure should truly be "exceptional", meaning there is a significant and possibly irreparable infringement of data subjects' rights and freedoms pursuant to the GDPR.

Data Protection Impact Assessments (DPIAs) and High-Risk Processing

- The protections in the GDPR for "high risk processing," and the DPIA procedure, both have the potential to significantly benefit data subjects – but both also risk creating disproportionate administrative burdens if guidance about these measures lack pragmatism.

- As a first step, there should be additional context provided regarding what constitutes "high risk processing," for example through factors or criteria that data controllers can take into account when conducting their internal assessments. These criteria should be based on evidence that relevant processing carries a risk of serious and irreparable harm.

- In addition, when considering risk, DPAs should bear in mind that the GDPR subjects *all* controllers, whether engaging in high risk processing or not, to significant supervision, duties to put in place appropriate data protection measures and follow privacy by design and default principles, with harsh penalties for breaches. These protections limit the scenarios where there will be a genuine and proportionate need for the additional protections reserved for "high risk" situations.

- To further reduce uncertainty, routine business operations should generally be whitelisted as not being "high risk".

- In terms of how DPIAs are done, organisations should be permitted to carry out DPIAs with flexibility. DPAs should avoid specifying DPIA content, format, frequency, etc. (beyond what is already in the GDPR); instead, businesses need to remain free to exercise their judgment to match the context of the processing. This reflects the "accountability" principle that is an underlying principle of the GDPR as a whole (see article 5).

- The "prior consultation" process should be required only where strictly relevant, and should be implemented in a manner that minimises disproportionate disruption to business. The Regulation is clear that prior consultation is only triggered when the data controller determines a particular type of processing qualifies as high risk, but is unable to mitigate these risks to data subjects.

- We look forward to guidance from DPAs and the future EDPB on a number of key issues on this procedure, in particular including our views that: (i) a DPA should clearly advise when a procedure is over; (ii) only the lead DPA should be consulted when processing has a multi-national scope, and (iv) prior consultation eliminates the need for an urgent consultation process (e.g. for small, one-off but potentially high-risk and time-critical processing operations).

Personal data breaches and notification

- GDPR requires notice to DPAs of a data breach "without undue delay," unless the breach is "unlikely to result in a *risk* to the rights and freedoms of individuals" and notice to data subjects where a breach is likely to result in a "high risk" to their rights and freedoms. Notification is not required if the data is secure (e.g., encrypted) or if the risk has been mitigated.

- Guidance is therefore needed regarding the types of breaches that create a "risk" requiring notice to DPAs, and what additional factors create a "high risk" requiring notice to data subjects. Without more objective standards, data subjects could receive notices so frequently that they become

unable to distinguish between those that reflect significant risk and those that reflect minimal or no risk, rendering notices ineffective.

- We suggest that guidance should include at least the following factors: (i) nature and extent of the Personal information (PI) involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorised person who used the PI or to whom the disclosure was made; (iii) whether the PI was viewed or acquired, (iv) the extent to which the risk to the PI has been mitigated.

- In addition, guidance is needed on which DPA needs to be notified of the breach in cases where a breach involves several Member States.

- Finally, guidance is needed for recordkeeping requirements particularly where little or no risk is likely to arise from the breach.

Approved Codes of Conduct and Certification

- Well-designed codes and certifications have the potential to set high standards of practice across industries.

- At the same time, codes / certification schemes must be pragmatic and flexible. Compliance with such schemes should also be affordable, in order to encourage industry to embrace them. They should set out examples of approved ways of complying with requirements, but should avoid highly granular criteria and should not favour certain business models over others.

- The negotiation procedure mechanism should allow for fluid interaction between the representatives of the code and the EDPB rapporteur as opposed to a static written procedure. In the case of the Data Protection Code of Conduct for Cloud Service Providers, it would have helped for a more timely adoption.

- Codes / certifications should also interoperate, wherever possible, with international practice, to prevent market fragmentation and avoid divergences among global privacy and security practices.

- Once a code / certification is approved, DPAs, the EDPB and the Commission should work together to incentivise adoption. However, codes and certifications should always remain voluntary.

Data Portability

- The right of data portability should help to enable the free flow of data across the EU. However, as the right of data portability is new, guidance will be helpful. Such guidance should clarify that the right covers only data provided by data subjects – for example, data filled in by the data subject in data entry fields like their name or address – but not data generated by the service, such as metadata about the use of a service, telemetry data about the operation of the service in general, or data that is inferred about a data subject by the company.

- Guidance should also clarify that "technical feasibility" excludes scenarios where new systems or capabilities would need to be built in order to enable direct exchange. Likewise, to enable companies to begin developing compliance procedures and capabilities, AmCham would welcome

clarifications as to how the phrase "structured, commonly used and machine-readable" will be interpreted. Our view is that such formats should be limited to only the most popular and common standards for structured documents and web data, potentially with other formats used only where data cannot be expressed through these formats.

Sanctions

- Sanctions should be given if there is a clear breach, and can deter bad practices within companies. At the same time, they are only effective if they are meaningful. Some of the most effective European regulators make extensive use of warning letters and other "soft" enforcement measures prior to, when necessary, imposing formal sanctions.

- The balanced use of a full spectrum of powers, and dialogue with industry, should be endorsed by the EDPB in order to create a harmonised and proportionate enforcement environment. This is particularly true and necessary considering that when the GDPR will start to apply, guidance will not be available to cover all aspects. Accordingly, we believe some leniency will be required until the DPAs and EDPB have issued guidance that is comprehensive and adequate to back up the GDPR sufficiently and clarify its intended application.

- The EDPB should also clarify that fines should account for whether an individual or entity has been subject to sanctions in another proceeding for the same conduct, so that a party is not penalised twice for the same conduct.

Data Protection Officers (DPOs)

- DPOs will enhance business accountability. But key concepts in the GDPR are unclear. Guidance should clarify, in particular, the meaning of the terms "core activities" and "large-scale processing," as used in Article 37. Policymakers could, for instance, specify that certain activities do not require DPO appointment, e.g. routine recruitment and HR practices, a company's use of cookies to monitor its own websites, or standard use of everyday business contact information (e.g. for customer relationship management (CRM), marketing or contract performance purposes).

- Guidance could also clarify other issues relating to DPOs, including how they should maintain their independence (and whether they can be held accountable to management and boards for performance); how SMEs should approach the issue of appointing DPOs; and whether DPOs can be external bodies and legal entities. Industry should be consulted to help produce best practices and working examples to provide further clarity.

- In order to promote innovative business models and operational flexibility, in particular for large businesses that operate across many jurisdictions globally, guidance should clarify that data protection officers can be located everywhere within the EEA.