AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Consultation response

Feedback on the report on the application of the General Data Protection Regulation

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 U.S. positions on business matters. Aggregate U.S. investment in Europe totalled more than €3 trillion in 2019, directly supports more than 4.8 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
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

The American Chamber of Commerce to the European Union (AmCham EU) has closely followed and participated in the discussions on the General Data Protection Regulation (GDPR) throughout its legislative adoption process and now looks forward to providing feedback to the upcoming Report on the application of the GDPR since its 25 May 2018 entry into application. AmCham EU represents a unique voice on data protection issues: our member companies operate across different sectors and value chains. They have a legal presence in multiple Member States and depend on stable intra-EU and international data flows. For AmCham EU's views, please consult below.

On international transfers of personal data to non-EU countries (Chapter V)

The modern economy is dependent on cross-border data flows. The ability to transfer personal data across the Atlantic and globally is essential for the competitiveness of many sectors. The GDPR has dedicated a complete chapter on cross-border data transfers and has institutionalised a number of transfer solutions to enable them. For some third countries, data protection adequacy decisions, such as for Japan, present an opportunity to increase trade. Obviously, adequacy of third countries provide businesses that rely on cross-border data flows the highest level of legal certainty. However, as not all countries follow the GDPR approach, alternative instruments and mechanisms, such as the EU-US Privacy Shield and standard contractual clauses (SCCs), continue to be essential for global trade.

AmCham EU took note of the EU's Advocate General Opinion concerning SCCs from December 2019 and is looking forward to the ruling of the Court of Justice of the European Union (CJEU). Further to that ruling, we urge the Commission to release revised SCCs aligned with the GDPR and with any guidance the ruling may contain to strengthen SCCs and make them a robust mechanism for international data flows going forward. These revised SCCs should also cover all transfer scenarios faced by businesses in a modular manner (controller-to-controller, controller-to-processors, controller-to-processor-to-sub-processor, processor-to-processor, etc.) with a sufficient period for companies to allow for a smoother transition phase. The new version of SCCs should also not have retroactive effects. In the worst-case scenario, where the CJEU would rule against the legality of SCCs as an alternative transfer mechanism, we look forward to the swift implementation of an alternative solution with practical guidance for businesses to ensure an uninterrupted flow of data with minimal impact on trade. All AmCham EU members work diligently to comply with the GDPR when transferring data outside of the EU, but require legal certainty and proper rules to implement and enable compliant data transfers. This ensures businesses can operate globally and can legally transfer data, thus enabling the digital economy to prosper, which is one of the core goals of the GDPR.

Likewise, the EU-US Privacy Shield, endorsed by the Commission after careful analysis of the US legal regime, remains an important mechanism for data flows and is relied upon by over 5,000 European and US companies. Support for the EU-US Privacy Shield should be reiterated by the Commission in its Report, including encouraging EU Data Protection Authorities (DPAs) to also voice their support for the framework.

With regard to binding corporate rules (BCRs), they are now fully recognised by the GDPR and apply throughout all EU Member States. They are also often considered as the 'golden mechanism' to enable cross-border data flows within a multinational group. Nevertheless, their review and adoption process remains unnecessarily burdensome and lengthy with a clear lack of resources at the DPA level. We would also insist on having the process more streamlined for both BCRs for controllers and BCRs for processors, whether or not combined.

The GDPR foresees alternative transfer mechanisms (Article 46), including certifications mechanisms and codes of conduct. Unfortunately, their uptake and adoption has been limited. Although the Commission supports their development as a viable alternative to other transfer mechanisms, we express our concern over the limited progress made to ensure they become a concrete alternative solution.

Moreover, it is unclear how organisations subject to the GDPR should deal with data transfers to the UK after Brexit. A timely adequacy recognition would ensure the highest level of certainty for businesses across the

Channel. As an alternative, regulators should issue guidance on how these data flows should be managed going forward to enable businesses to put plans in place prior to 31 December 2020.

On the cooperation mechanism between national data protection authorities (Chapter VII)

AmCham EU supports a uniform and balanced application of the GDPR across Europe. One of the main goals of the GDPR is to achieve greater harmonisation in data protection rules and practices across the EU in favour of the Single Market and in order to make business more efficient, improve legal certainty and provide data subjects with the same protection across the EU. It must also be ensured that future privacy frameworks as the ePrivacy regulation are aligned with the GDPR as conflicts would create a high degree of legal uncertainty. The European Data Protection Board (EDPB) has a crucial role to play in this regard. Its guidance has been important in helping companies understand their compliance obligations. However, uncertainty has been triggered by diverging interpretations with guidance that sometimes goes beyond what the GDPR prescribes. This is regrettable and limits the benefits that harmonised rules would provide.

We fully support the cooperation mechanism that has been put in place among the DPAs to avoid divergent interpretations of similar issues. The cooperation and consistency mechanism is a core principle of the GDPR to avoid the fractured nature of data protection enforcement across Europe under the old legal regime for organisations involved in cross-border processing operations. Businesses must have the certainty that they only need to deal with one supervisory authority for cross-border processing. This, together with the simplifications brought by a single Regulation was due to lead to savings estimated at EUR 2.3 billion per year.[1] As new technologies are developing, further questions about the interpretation of the GDPR will emerge and finding solutions will require a continued dialogue between regulators and industry stakeholders.

One essential element to achieve harmonisation is the One-Stop-Shop mechanism. In fact, one of the main reasons for the proposal of the GDPR was the promise of a harmonised approach to data protection, both in terms of substantial law and enforcement.[2] It is therefore essential that the rules around cooperation between DPAs are fully respected to ensure that DPAs are interpreting the GDPR in a harmonised way and that enforcement proceedings are taking place in accordance with the mechanisms described in the GDPR. Since the entry into application of the GDPR, the One-Stop-Shop mechanism has been weakened by the fact that some DPAs are departing from that principle. It should be recalled that the One-Stop-Shop mechanism does not preclude other DPAs from participating in the decision-making process through the cooperation procedures as described in Article 60 of the GDPR. Therefore, DPAs should be encouraged to actively participate in the decision-making process via these procedures rather than by initiating their own proceedings on an individual basis, be it against the local establishment or the main establishment without consideration of its identified lead authority in a cross-border situation.

As far as enforcement is concerned, DPAs should be encouraged to come up with a single set of enforcement and sanctioning rules. More generally, where the GDPR does not allow for individual national approaches, DPAs should not come up with their own interpretation but rather support the EDPB to provide a uniform one. This could include a common model for calculating fines. Another illustration is the interpretation by the Dutch DPA of the legitimate interests as a legal ground for processing (Article 6) which, in our view, contradicts the GDPR to the extent it considers that the processing of personal data for purely commercial interests and profit maximisation does not pass the 'legitimacy' test.

The Dutch DPA's view differs in that respect from the opinion of the Article 29 Working Party on legitimate interests (Opinion 06/2014) and other DPAs where 'the notion of legitimate interest could include a broad range of interests, whether trivial or very compelling, straightforward or more controversial. It will then be in a second step, when it comes to balancing these interests against the interests and fundamental rights of the data subjects, that a more restricted approach and more substantive analysis should be taken'. This difference is very

[1] 'Joint Statement on the final adoption of the new EU rules for personal data protection'. https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_16_1403

[2] This is confirmed by emerging GDPR case law (Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein GmbH* and *Case Google LLC v CNIL*)

likely to lead to different outcomes in the Netherlands than elsewhere in the EU. This is also valid with regards to the statement of the Dutch DPA on data usage to ensure employees' health during the COVID-19 crisis.[3] Health data (eg, resulting from temperature checks) might be invaluable to guarantee a safe return to workplace, given the specific safeguards of the GDPR are met. Clarity on the legal basis would also be helpful in other contexts, such as access to domain name registrant data (also known as WHOIS data) that has been made largely inaccessible since May 2018, even for purposes of law enforcement, IP rights enforcement and consumer protection to the detriment of the public interest and a measurable negative impact on cybersecurity.

The role of the EDPB is essential here. The EDPB must ensure that the harmonisation promise is kept and that DPAs are on the same page. In order for the EDPB to complete its tasks efficiently, its procedures and website should be made more transparent (without prejudice to protecting sensitive information, eg in the context of BCR review). This includes better transparency on mandates, information on which DPAs are involved in drafting guidance, structures of the working groups and timelines for adoption of documents.

Conclusion

Due to all of the above, we welcome the reaffirming of the rules regarding the cooperation and consistency mechanism. Any attempt to circumvent the above mechanism would be detrimental to business certainty and investment in the EU. The success of the GDPR for citizens, consumers and businesses will require a constructive exchange amongst the EDPB, national DPAs and industry stakeholders. AmCham EU looks forward to the forthcoming Commission report and to continuing the dialogue.

[3] https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-temperatuur-meten-mag-niet-zomaar?utm_source=POLITICO.EU&utm_campaign=1ce5ad6d93-EMAIL_CAMPAIGN_2020_04_27_05_00&utm_medium=email&utm_term=0_10959edeb5-1ce5ad6d93-190137589