U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

February 8, 2024

Olivier Micol
Unit C.3 Data Protection
Directorate General for Justice and Consumers
European Commission

Bruno Gencarelli
Unit 01 International Affairs and Data Flows
Directorate General for Justice and Consumers
European Commission

Re: U.S. Chamber of Commerce Response to the European Commission on the Implementation of the General Data Protection Regulation

Dear Mr. Micol and Mr. Gencarelli:

The U.S. Chamber of Commerce ("Chamber") welcomes the opportunity to provide comments on implementation of the General Data Protection Regulation ("GDPR").

The Chamber is the world's largest business advocacy organization, promoting free enterprise and advancing American trade and investment globally. In Europe, we work closely with our partner organizations at AmCham EU, American Chambers of Commerce in all 27 member states, and with our counterparts at BusinessEurope and other member state business organizations.

The GDPR has reshaped how companies around the world do business in or trade with the European Single Market. While the regulation is proving beneficial in some respects, five-plus years of implementation have also provided insight into how it can be improved.

Exercise of Data Subject Rights

The GDPR grants data subjects' expansive rights in the areas of data access and portability. Developing systems to comply with these rights is not only costly but comes with counterbalancing risks and may strain the bounds of what is technically feasible. For example, providing "all instances" of personal data may lead to an overwhelming "data-dump" of repetitive low risk data that customers cannot comprehend. Further, "porting" such data may in fact engender data security risk. The

European Data Protection Board ("EDPB") and Data Protection Authorities ("DPAs") have not provided sufficient practical guidance on how to resolve the tensions between data protection and other interests. Faced with a lack of clarity on the expected controls under the Accountability Principle and how they may evolve, companies are in a difficult position They must guess how to comply with the law and face harsh penalties if their good faith attempts fall short. The sanction is particularly disproportionate where there is no substantive privacy harm to the data subject as well as considering unintended circumstances where such rights have been invoked (e.g., as a discovery tool or form of harassment in employment litigation).

Experience with Data Protection Authorities

DPAs often are unwilling to provide tailored guidance, which is needed given the horizontal and principles-based nature of the GDPR, based on professed resourcing constraints. The EDPB should create a framework for data controllers to voluntarily reach out to DPAs in good faith, and the DPAs should play a more proactive role in engaging with other regulators to clarify their areas of competence to avoid potentially conflicting rulings. Member states must also ensure that DPA's are appropriately resourced.

Data Protection Officers (DPOs)

The requirement to appoint a Data Protection Officer ("DPO") helped to ensure organizations that traditionally did not have staff responsible for data protection would integrate one into their structure to assist with GDPR compliance. While the DPO can serve as a useful bridge between an organization and regulatory authorities, there is a risk that terms for designating this person are too prescriptive. In particular, there are counterbalancing requirements in the GDPR for the DPO to be "conflict free" but also "informed" and "appropriately qualified."

In practice, these requirements can mean that DPOs are not senior individuals well positioned to appropriately comment on the business practices under discussion with suitable sophistication. This is particularly true if DPAs begin to assert that in fact a conflict exists merely because a DPO is a member of either management or even the legal department. Indeed, DPAs should not read hard additional requirements into GDPR that do not exist in the text, but instead must provide suitable discretion for companies to operate within the spirit of the legislation. It is essential that discretion be given to data controllers in appointing their DPOs. DPAs should acknowledge that there is not a "one size fits all" solution for the DPO role and should provide suitable deference in application of the requirement.

Controller/Processor Relationship (Standard Contractual Clauses)

Under European Court of Justice case law, the data controller must undertake a Data Transfer Impact Assessment when using Standard Contractual Clauses to analyze the risks of the transfer. The details of the Transfer Impact Assessment are not set forth in GDPR, yet the EDPB guidance remains impractical when considering the multitude of required use cases. Future guidance must consider what is practically feasible versus a "best of all worlds" solution.

International Transfers

GDPR requires that data transfers from the EU to the U.S. be grounded in mechanisms such as model clauses promulgated by the European Commission or the EU-U.S. Data Privacy Framework.

While mandating certain safeguards where organizations transfer data out of the European Economic Area is understandable, many of the solutions favored under the GDPR (e.g., model clauses) have resulted in onerous administrative burdens. These burdens take years for approval, and it is unclear whether the tangible benefits for data subjects are proportionate to this cost. It is also not appropriate for companies to risk turnover fines despite acting in good faith.

- The interruption of international data flows that we have seen between the EU and U.S. is not sustainable. The high level of legal uncertainty also carries a risk of high fines for organizations transferring data outside of the EU, despite acting in good faith and within the framework of the EU's adequacy decision.

- As for binding corporate rules ("BCRs"), the administrative procedure should be simplified, comparable to Standard Contractual Clauses, to enable accountability and transparency.

- GDPR certifications and codes of conduct have potential value as comprehensive accountability mechanisms. While the regime surrounding GDPR certifications and codes of conduct have still not been set up, there is positive potential in implementing these tools. Although no scalable means of implementation currently exist, we encourage their realization.

Fragmentation/Use of Specification Clauses

The GDPR aims to harmonize data protection rules in the EU, yet this goal has been difficult to achieve. Member states' differing interpretations of the GDPR have led to divergent rules in practice. For example, DPAs have adopted various positions

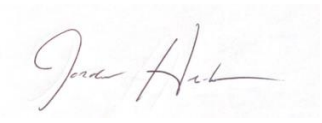
on the requirement of a Guest Check Out feature for online shopping. The EDPB could play a more active role in driving true consistency in the way DPAs interpret and approach data protection rules, compliance, and enforcement while also ensuring that DPAs do not take on a quasi-legislative remit by overstepping GDPR requirements. Cookie consent requirements are another case in point, varying across member states in how to obtain valid consent from users for storing or accessing cookies and other tracking technologies.

GDPR and Innovation

Although the GDPR is intended to be future-proof and adaptable to emerging technologies and new uses of data, this is not entirely the case. Several provisions may not be appropriate for artificial intelligence applications, developing biotechnology, and blockchain. Moreover, the overlap between GDPR and sector-specific legislation can create conflict, leading to significant ambiguities regarding the intersection of GDPR with measures such as the e-Privacy Regulation, Digital Markets Act, and the EU AI Act. A risk-based approach to the GDPR would permit the GDPR to stay future-proof and continue to adapt to new technologies. For the future, guidance and exchange is needed by the Commission, the EDPB, and other relevant regulators to provide workable and scalable guidance to economic operators. Additionally, legislative proposals from the Commission must carefully consider potential areas of contradiction and overlap.

We stand ready to discuss these matters further with the Commission. Please contact Zach Helzer zhelzer@uschamber.com for additional information. Thank you for your consideration of our views.

Sincerely,



Marjorie Chorlins
Senior Vice President, Europe
U.S. Chamber of Commerce

Jordan Heiber
Vice President, International Digital Economy
U.S. Chamber of Commerce