December 18, 2020

U.S. Chamber of Commerce Response to the European Data Protection Board's *Recommendations on Measures that Supplement Transfer Tools to Ensure Compliance with EU Level of Protection of Personal Data*

On behalf of the U.S. Chamber of Commerce, we are pleased to provide comments on the European Data Protection Board's *Recommendations on Measures that Supplement Transfer Tools to Ensure Compliance with European Union Level of Protection of Personal Data* ("Recommendations").

The U.S. Chamber of Commerce ("Chamber") is the world's largest business federation, representing more than three million enterprises of all sizes and sectors. The Chamber is a longtime advocate for strong commercial ties between the U.S. and the European Union and is a leading business voice on digital economy policy, including on issues of privacy, cybersecurity, and digital trade. In the U.S., Europe, and globally, we advocate for sound policy frameworks that support economic growth, promote data protection, and foster innovation. Many of the Chamber's members are heavily invested in the EU, which also represents a major U.S. export market.

The continued flow of personal information from Europe is essential to Europe's competitiveness and connectivity to the global economy, as well as to research that is critical to fighting and recovering from the current pandemic. Given the legal questions raised by the Court of Justice's ("Court") decision in case C-311/18, the Chamber welcomes efforts by the European Data Protection Board ("EDPB") aimed at enabling businesses to continue transferring EU personal information with confidence and in compliance with European law. In this respect, we thank the EDPB for granting our November 12 request to extend its public consultation period.

Unfortunately, the Recommendations, as written, fail to provide businesses with a realistic way forward on international data transfers. The EDPB's proposed measures are unworkable in practice, go beyond the requirements laid out by the Court, and are inconsistent with the *General Data Protection Regulation*'s ("GDPR") risk-based approach

to data privacy. If the Recommendations are implemented and enforced as written, the EDPB will effectively cut Europe off from the rest of the digital world and erect formidable barriers to cross-border trade and investment, without enhancing the privacy of European citizens.

We urge the EDPB to fundamentally reconsider its proposals. It should embrace a risk-based approach that enables enterprises to choose supplementary measures that are appropriate to the contexts of their data transfers. Such an approach would remain consistent with the Court's decision and the GDPR and should be coordinated with the European Commission's new standard contractual clauses ("SCCs"). We further recommend that the EDPB include a transition period that allows for enterprises to adjust their business arrangements to comply with the new requirements. Given the economic and social challenges stemming from the COVID-19 pandemic, the EDPB must avoid creating unneeded disruptions to cross-border commerce. Our concerns and recommendations are detailed below.

I. The Recommendations are a *de facto* data localization requirement

The Chamber recognizes the importance of the EDPB's task of bringing the EU's international data transfer regime in line with the Court's decision in C-311/18. In doing so, however, the EDPB must acknowledge that cross-border transfers of personal information are integral to the day-to-day operations of most organizations in Europe. Businesses of all sizes and in sectors as diverse as healthcare, transportation, hospitality, retail, information technology, logistics, and financial services routinely access globally delivered services and transfer data to conduct cross-border commerce and research. According to a recent survey by the European business community, more than 85 percent of these organizations rely on SCCs to transfer personal information out of Europe, with 90 percent of transfers taking place between businesses.[1] These flows are crucial for an estimated €550 billion of digitally enabled services annually exported by the EU to the rest of the world, as well as for the global scientific effort to combat the COVID-19 pandemic.

The EDPB's Recommendations fail to accommodate such realities. First, the proposals prohibit European personal information from being transferred to or accessed from "non-adequate" jurisdictions when it is, at any point, "in the clear." Organizations that cannot comply must immediately cease their transfers, return the personal information to the EU, and destroy any copies held abroad. This means that European personal information must *always* and at *all times* be encrypted or pseudonymized when in a "non-adequate" jurisdiction *and* the cipher (e.g., encryption

[1] BusinessEurope, European Roundtable for Industry, et al, *Schrems II Impact Survey Report*.

key) must be held in the EU or another jurisdiction that is deemed "adequate." This is an unreasonably high technical threshold for organizations to meet and restricts commercially meaningful and otherwise routine practices that rely on cross-border data flows. Second, the Recommendations explicitly invalidate common business arrangements, namely the use of cloud computing to process "data in the clear" and remote access to data for business purposes (e.g., human resources). Taken together, these proposals serve as a *de facto* localization requirement for EU personal information. U.S.- and other foreign-headquartered companies would be required to cease international data transfers and either localize their storage and processing in the Single Market or cease doing business there altogether.

The Recommendations suggest that everyday transfers of personal information may result in GDPR violations. These include routine communications between colleagues across borders, researchers and public health officials sharing data to fight COVID-19, and financial services firms leveraging global platforms to detect and combat fraud and money laundering and to maintain operational resilience, which is needed to uphold the safety and soundness of the global financial system. Restrictions on the flow of personal information will obstruct the cross-border provision of cybersecurity services to the European Union, cutting it off from information security talent outside of the Single Market. It would also obstruct the flow of cyber threat information from the EU to the rest of the world, as organizations would have difficulty alerting EU authorities to malicious activity originating in Europe.[2] Consequently, the data protection of EU citizens and its trading partners would suffer.

In transforming the EU into a "digital island," the Recommendations would cause significant disruptions to international commerce and to the goods, services, and research that Europeans rely on. They may also disincentivize foreign firms from employing EU citizens or investing in Europe, as companies may be unable to transfer EU employee data in a personally identifiable form to their headquarters or global services centers outside of Europe. Furthermore, the EDPB's measures would undermine the ability of EU institutions and member states to pursue a range of other legitimate public policy objectives, such as transatlantic law enforcement and security cooperation, which often benefits from the ability of companies to identify bad actors and notify authorities, resulting in prosecutions.[3]

---

[2] IP addresses, which are central to cyber threat information sharing, have been treated as personal information under the *General Data Protection Regulation*.

[3] The U.S. Treasury's Terrorist Finance and Tracking Program ("TFTP") regularly provides Europol and EU member states with information needed to investigate terrorist attacks and plots, including many of the most infamous in recent memory. The TFTP, whose privacy safeguards are reviewed by the U.S. Privacy and Civil Liberties Oversight Board, relies on transfers of personal information from servers located in Belgium. While the TFTP rests on a bilateral agreement between the U.S. and EU, it is difficult to foresee how a partnership such as this—which is grounded in

A *de facto* data localization requirement will have spillover effects in other areas, including public health, as multi-country clinical trials, pharmacovigilance efforts, and pandemic monitoring and response all rely on cross-border transfers of personal information. According to a forthcoming report from the Information Technology & Innovation Foundation, in October 2020, there were 1,322 active clinical trials involving organizations in the United States and the twenty-seven EU member states, which represents 39 percent of active clinical trials registered with the U.S. Food and Drug Administration.[4] This includes studies related to COVID-19, as well as treatments for cancer, arthritis, asthma, HIV infections, lupus, epilepsy, and other diseases. While the Chamber broadly agrees with Chair Andrea Jelinek's statement earlier this year that "data protection rules do not hinder measures taken in the fight against the coronavirus pandemic," the EDPB's latest proposals may inflict significant harm on public health and the transatlantic life sciences ecosystem.[5]

II. The Recommendations are prescriptive and not in line with the GDPR and the CJEU's decision in C-311/18

The transfer of personal information across borders takes different shapes and forms, involves different kinds of data, different purposes for processing, and different recipients in different locations. Importantly, Chapter V of the GDPR recognizes the contextual nature of data transfers and offers organizations a range of risk-based tools from which to choose. Article 46 *explicitly* requires organizations to choose "appropriate safeguards" for their transfers of personal information out of the European Union. This is in keeping with the GDPR's broader risk-based framework. The GDPR states that the implementation of *appropriate* technical and organizational measures depends on a *risk assessment* that factors in the sensitivity of the data, likelihood of access, and risk of harm to data subjects if accessed.[6] Similar evaluations of risk guide controllers in their selection of processors, in the performance of data protection impact assessments, and in determining the extent of breach reporting that is required.[7] The Court affirmed this approach in C-311/18, stating that organizations must make "case-by-case" assessments, and that "all the circumstances" must be considered when determining whether an organization can proceed with a data transfer.[8]

By contrast, the Recommendations outline a six-step assessment that organizations must meet to transfer Europeans' personal information abroad. This

values shared on both sides of the Atlantic—will not be disrupted by the EDPB's proposed regulatory standards. See U.S. Treasury, *Terrorist Financing Tracking Program* and U.S. PCLOB, *Chairman's Statement on TFTP*.

[4] Forthcoming report from Nigel Cory, Information Technology & Innovation Foundation.

[5] European Data Protection Board, *Statement by EDPB Chair on COVID-19*.

[6] *General Data Protection Regulation,* Article 32, Recitals 78 and 83.

[7] GDPR, Articles 33 to 35, Recitals 81 to 91.

[8] Court of Justice of the European Union, *Case C-311/18*, paragraphs 131 to 134.

prescriptive approach contravenes the GDPR's principle of accountability and fails to account for the costs of compliance.[9] Compliance burdens fall especially hard on small and medium sized enterprises, for whom *existing* European data protection requirements already pose a formidable barrier to doing business in the Single Market. The EDPB states that organizations must adopt supplementary measures any time there is a *theoretical possibility* that EU personal information may be accessed by the government of a "non-adequate" jurisdiction. This remains the case even, presumably, if organizations receiving EU personal information have never faced a lawful order to provide such data and the data is of no conceivable relevance to national security. The EDPB's Recommendations suggest that "subjective" considerations such as these are irrelevant, a position that is out of line with the GDPR's risk-based framework. The U.S. Government, a mutual defense treaty ally of European member states and Europe's primary security and law enforcement partner, has publicly stated that "most U.S. companies do not deal in data that is of any interest to U.S. intelligence agencies."[10]

The Recommendations not only require organizations to apply safeguards where there is a theoretical possibility of access; they state, as a general matter, that organizational and contractual measures are insufficient to overcome access to EU personal information by third-country governments. Consequently, only technical measures (e.g., encryption) will meet the EDPB's proposed standard, regardless of the transfer and the level of risk involved. This heavy-handed, "one-size-fits-all" approach would effectively ban common business arrangements, even as such a theoretical danger could occur within the EU as well. In Use Cases 6 and 7, for example, the EDPB states that it is "incapable of envisioning an effective technical measure" for transfers to cloud service providers or other processors which requires access to "data in the clear," as well as for remote access to data for business purposes. Countless organizations engage in these practices. Foreign companies invested in the EU, for example, routinely transfer the human resources data of their European employees to headquarters in "non-adequate jurisdictions," such as the United States and India.

The EDPB's invalidation of these arrangements insufficiently accounts for the deleterious effect that it will have on other fundamental rights guaranteed under the *Charter*. These include the right to liberty and security, rights related to free expression, access to information, and assembly, and economic rights and freedoms, such as the right to employment and to own a business.[11] All are supported, if not effectuated by, transfers of EU personal information with the rest of the world.

---

[9] GDPR, Article 5.

[10] U.S. Department of Commerce, U.S. Department of Justice, and U.S. Office of the Director of National Intelligence, *Information on U.S. Privacy Safeguards Relevant to SCCs and other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*.

[11] Cf: *Charter of Fundamental Rights of the European Union*.

III. The EDPB's standard for technical measures is unworkable

The EDPB's standard for technical measures is unworkable as a threshold for international data transfers. The Recommendations clearly establish encryption as the preferred supplementary measure. In the EDPB's eyes, however, encryption is only sufficient if the data never appears in an unencrypted form in a third country *and* if the cipher is held only within the EU or an "adequate" jurisdiction. Yet *any use of data*, such as sending emails or texts, processing customer payments, or engaging in business transactions, requires data be available in a decrypted format. Other technical measures, such as pseudonymization, may allow for subsequent data analysis but rule out the processing of EU personal information for business purposes such as human resources. "Split processing," meanwhile, would not appear to be available for most enterprises. If such extreme measures were applied to transfers regardless of risk, in many cases, transfers would be impossible altogether.

The Recommendations also advise that, to be sufficient, technical measures must impede all government access to data, including through encryption of data that is "flawlessly implemented" and resistant to cryptanalysis. It is unclear how a company can verify that it has "flawlessly" implemented encryption, and effectively prevented a foreign government, with all its resources, tools, and computing power, from deciphering encrypted EU personal information. Likewise, the proposal that businesses use technical measures to create "obstacles for attempts from public authorities to access data" is excessive and ignores legitimate concerns by enterprises regarding conflict of laws between different jurisdictions in which they operate. Using technical tools like encryption is a good practice to safeguard data confidentiality from malicious actors and to protect privacy; however, recommending that companies blind themselves to all EU personal information in order to obstruct compliance with lawful requests from foreign governments not deemed "adequate," including the U.S., is both untenable and disproportionate, as it is disconnected from the realities of cross-border commerce.[12]

IV. The Recommendations will hinder, rather than advance, cooperation among democratic governments on privacy and lawful access to data

The EDPB's Recommendations rest on the erroneous assumption that international transfers are necessary for governments to access European personal information. Governments, European and foreign alike, can access EU personal

[12] U.S. Chamber of Commerce, *Statement on Encryption and Cybersecurity*.

information *in Europe*, without commercial cross-border data flows. The Chamber also notes that European policymakers are seeking greater access to encrypted data at rest and in motion for matters of law enforcement and public security.[13] As in its *Recommendations on European Essential Guarantees for Surveillance Measures*, the EDPB's proposals risk holding foreign jurisdictions to a higher standard than European institutions and member states. The example of the United Kingdom underscores this inconsistent standard.[14] Transfers of EU personal data would not be in question if the UK remained within the European Union. Only after its departure from the EU has its legal framework for government access to data been subject to scrutiny for the purposes of cross-border data flows.[15] Asymmetries such as these hinder, rather than support, cooperation between the EU and democratic allies on issues of privacy and lawful government access to personal information.

The EDPB should consider the ramifications of implementing its Recommendations, as well as the numerous safeguards that may be applied in response to realistic assessments of risk. The Chamber urges the EDPB to uphold strong encryption as integral for individual and enterprise cybersecurity *and* to support robust international engagement on common frameworks for privacy and government access to data in a democratic society. Discussions at the Organization for Economic Cooperation and Development can serve as one avenue for advancing these frameworks. At the same time, measures that restrict data flows will prove counterproductive to cooperation with democratic allies and is at cross-purposes with European efforts to reenergize transatlantic relations and foster a more pragmatic and cooperative EU-U.S. policy agenda.

V. The EDPB should embrace a pragmatic way forward

The Chamber encourages the EDPB to reevaluate its Recommendations and reorient them so that enterprises have the flexibility to choose supplementary measures that are appropriate to the context of their data transfers. Rather than discouraging businesses from considering contextual factors, the Recommendations should *encourage* them to account for real-world (i.e. "subjective") risks of a transfer, including the relevance of the data to foreign governments and the frequency and likelihood of such agencies' access to the data. If these real-world risks are low, the supplemental measures organizations are expected to adopt should be appropriately narrowed. The

---

[13] European Council Declaration on Encryption, *Security Through Encryption and Security Despite Encryption*.

[14] See Patel and Lea, *EU-U.S. Privacy Shield, Brexit, & the Future of Transatlantic Data Flows*, pages 31-32.

[15] The UK *Data Protection Act* is transposed from the GDPR, is enforced by the highly regarded Information Commissioner's Office, and, for the purposes of commercial data privacy, should be considered "essentially equivalent."

Recommendations should also be clear that, in line with the principle of accountability, organizations are free to choose the data tools they deem most appropriate. This would entail putting organizational and contractual measures on equal footing with technical ones, as they can be effective to challenge unlawful government requests, for example.

The EDPB should coordinate its Recommendations with the new draft SCCs proposed by the European Commission, which themselves are subject to public comments and which have received considerable attention from the business community on both sides of the Atlantic. The EDPB's proposals should not attempt to pre-empt or limit their scope of application. Moreover, the EDPB and individual DPAs should refrain from imposing sanctions on companies until the new SCCs have been adopted, the Recommendations have been finalized, and a sufficient period of time has elapsed to enable businesses to implement the relevant procedures.

VI. Conclusion

If implemented and enforced as written, the EDPB's Recommendations will cause significant commercial disruptions, with few, if any corresponding benefits to the privacy of EU citizens. The Chamber therefore urges the EDPB to fundamentally rethink its Recommendations in the manner described above. We stand ready to work with you on these issues and appreciate your consideration of our views.

Contact Information

Marjorie Chorlins
Senior Vice President
European Affairs
U.S. Chamber of Commerce
mchorlins@uschamber.com

Sean Heather
Senior Vice President
International Regulatory Affairs
U.S. Chamber of Commerce
sheather@uschamber.com

EU Transparency Register: 483024821178-51