February 2024

Global Data Alliance's
Response to the European Commission's Call for Evidence on the Second Application Report of the EU General Data Protection Regulation

The Global Data Alliance[1] (GDA) is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The GDA supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. The GDA's members are headquartered across the globe, including the European Union, and are active in the advanced manufacturing, aerospace, automotive, consumer goods, electronics, energy, financial services, health, supply chain, and telecommunications sectors, among others.

The GDA welcomes this opportunity to provide input for the second report of application of the EU General Data Protection Regulation (GDPR). In this submission, the GDA will focus on particular issues related to international data transfers.

The GDPR has become a global point of reference at a time when many countries are developing or updating their privacy laws and regulations based on standards pioneered in the GDPR. Very importantly, the GDPR enshrined **free movement of personal data** as a crucial pillar of the EU acquis, supporting digitalization and streamlining data processing, thus facilitating the digital transformation of the economy. The overarching goals of the GDPR – to **provide high levels of data protection and ensure free movement of data** – are continuously essential to privacy laws worldwide. The principles that underpin the GDPR have been foundational to privacy legislation for decades and across economies. Offering these principles to all customers globally helps foster trust and transparency and contributes to reaching global convergence across privacy frameworks. The EU has a critical role to play to encourage international privacy best practices and interoperability of privacy systems.

I. International data transfers

GDA members appreciate the international data transfers' toolbox of the GDPR and support its strengthening to boost global data flows. Cross-border data flows are necessary for companies to operate globally and to provide services to their customers, across sectors and geographies.[2] The GDPR provides a list of mechanisms that can be used by organizations to comply with the Regulation's general principles and specific requirements when transferring personal data outside the EU. Different

[1] For more information on the Global Data Alliance, please see: https://www.globaldataalliance.org/. BSA | The Software Alliance administers the Global Data Alliance; EU Register of Interest Representatives: 75039383277-48
[2] https://www.globaldataalliance.org/downloads/GDAeverysector.pdf

organization types and business models require the use of different transfer mechanisms that are not interchangeable. **It is important that businesses would be able to use the full range of existing GDPR-compliant data transfer mechanisms**, such as: adequacy decisions (including on the EU-US Data Privacy Framework or EU-US DPF); certifications; codes of conduct; Binding Corporate Rules; and Standard Contractual Clauses. These mechanisms are critical to support global data flows and are built with strong safeguards.

The GDA supports the European Commission's work on **adequacy decisions** and believes they should be used more broadly. However, the process that determines whether a country is adequate remains too time consuming and should be accelerated: as of February 2024, the EU had finalized 16 adequacy decisions, including for commercial transfers to the United States through the EU-US Data Privacy Framework. As of February 2024, more than 2,600 companies from across the US have self-certified for the EU-US Data Privacy Framework, including GDA members. Many of the companies certified are small- or medium-sized businesses, across industries.

The GDA encourages the Commission to expand and speed-up adequacy decisions, considering their positive impact on the economy, and the growing digital trade between the EU and third countries. Thus, GDA embraces the European Data Protection Board's (EDPB) recommendation[3] to the Commission to *develop, expand and multiply adequacy negotiations with third countries* (in particular, the ones that play an important role in the global digital economy and to which a particularly large amount of personal data is transferred from the EU) and international organizations (whose legal frameworks are essentially equivalent to that of the EU). In addition, GDA members want to make sure that the EU-US Data Privacy Framework is a reliable permanent solution for transferring data between the EU and the United States and that it will stand the test of the European Court of Justice.

Among other data transfer mechanisms in the GDPR, EU lawmakers developed **Standard Contractual Clauses (SCCs)** so that organizations can transfer data to all the other countries whose regimes may not be recognized as essentially equivalent to that of the EU. In this case, the GDPR puts the burden on companies to apply strong safeguards when using the SCCs, so that data is protected at high levels wherever it travels. SCCs are an essential part of the day-to-day operations of companies across Europe, to transfer data with affiliates, vendors, customers and suppliers. According to a 2019 IAPP-EY report[4], approximately 88% of companies transferring data out of the EU rely on SCCs.

The GDA welcomes the European Commission's work in 2021 updating and revising the SCCs, and bringing them in line with the GDPR. GDA members recognize the positive impact of the updated SCCs. For example, Modules 1-4 of the updated SCCs have helped GDA members regulate relationships that were not covered in the previous SCCs (e.g. regarding P2P or P2C transfers). Clauses 14 and 15 of the updated SCCs have also ensured that the SCCs remain in line with the latest case law of the European Court of Justice (e.g. Schrems II judgment and the transfer impact assessment requirements stemming from this judgment).

However, GDA members' experience exposed some **challenges remaining in the updated SCCs**:

- Insufficiencies and areas of uncertainty remain with respect to *transfer impact assessments* (TIA). Clause 14 of the SCCs require Exporter/Importer carry out an in-depth *study of the legal framework of the territory* where the Importer is located. This triggers increased efforts in external

[3] EDPB "Contribution of the EDPB to the report on the application of the GDPR under Article 97": edpb_contributiongdprevaluation_20231212_en.pdf (europa.eu)
[4] IAPP-EY Annual Governance Report 2019, https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/

resources to examine foreign legislation. Some importers (i.e. SMEs) may not have the resources to undertake this obligation. In addition, these increased efforts may not be sufficient to address in enough detail the entire legal framework of a territory, as there is no guidance/threshold that allows exporter/importer to understand when a TIA will be considered enough/satisfactory for a Data protection authority (DPA). Although EDPB recommendations on supplementary measures have helped, uncertainty as to when a TIA will be considered sufficient before the eyes of a DPA still remains. In addition, the wording in Clauses 14 and 15 of the SCCs raise disputes in contract negotiations about who is responsible for conducting the TIA and whether the TIA needs to be shared with the other party.

- Likewise, DPAs have recognized *additional measures* going beyond the non-exhaustive list of technical, organizational and contractual measures set forth in the EDPB's supplementary measures guidance, i.e. solution of France's DPA involving a proxy server which avoids direct contact between a user's terminal and Google's server. It is however unclear whether the supplementary measures recognized/proposed by one DPA would be also recognized in all EU Member States.

Binding Corporate Rules (BCRs) are a tool of significant importance for companies, including some GDA members but their review and adoption processes are burdensome and lengthy for both companies and DPAs. DPAs and EDPB should dedicate sufficient resources to facilitate these processes. The GDA welcomes the updated EDPB's guidance on the BCRs for controllers, and encourages publication of the EDPB's guidance on the BCRs for processors.

GDA members believe that the **Codes of Conduct** could be a strong and valuable compliance tool. The European codes of conduct strengthen compliance with the GDPR and enhance trust among users and DPAs due to their pan-European scope. These codes undergo a specific review by all EU DPAs, with the issuance of an opinion by the EDPB at the conclusion of the procedure. Its adoption procedure makes the European codes of conduct a very valuable compliance tool which oversees application of the GDPR and reinforces trust. However, codes of conduct usually take years to be drafted and approved due to the complex requirements to be met and therefore the stakeholders are often discouraged to launch them. Drafting a code of conduct requires extensive consultation and exchanges among the stakeholders and it can take a very long time to align all parties. Among the challenges are also the differentiating interpretation of the provisions of the GDPR by various stakeholders. Therefore, to this day, codes of conduct, as well as certification mechanisms remain largely theoretical, hindering those willing to invest in such programs and thereby impacting public trust.

The GDA supports initiatives that make use of Article 46 of the GDPR to create **additional tools** to help address business needs in a legally and operationally sound manner, in line with the accountability principle. GDA members would welcome further certifications, including as they leverage existing international standards such as the Service Organization Control (SOC) 2[5] and ISO security standards. However, any such tool shall not include protectionist data localization requirements.

The misconception that **data localization** leads to better data protection is extremely dangerous. Data localization undermines the goals of the GDPR, which aim to ensure a high level of data protection and facilitate the free flow of data. GDA members' experience and recent research[6] show that GDPR-induced

[5] See ENISA's CCSL - Cloud Certification Schemes List: Cloud Computing Certification Schemes List - CCSL | Shaping Europe's digital future (europa.eu)

[6] Risks to Cybersecurity from Data Localization, Organized by Techniques, Tactics, and Procedures by Peter Swire, DeBrae Kennedy-Mayo, Drew Bagley, Avani Modak, Sven Krasser, Christoph Bausewein :: SSRN

data localization threatens the ability to achieve integrated management of cybersecurity risks and limits the ability to employ state-of-the-art cybersecurity measures that rely on cross-border data transfers to make them as effective as possible. This also clashes with the controller's and processor's obligation of Article 32 of the GDPR to "develop appropriate technical and organizational measures to ensure a level of security appropriate to the risk", "taking into account the state of the art". In addition, data localization undermines information sharing within industry and with government agencies for cybersecurity purposes, which is generally recognized as vital[7] to effective cybersecurity. ***A unified response by the EDPB and the European Commission expressing opposition to occasional calls by some DPAs to localize data should help promote the goals of the GPDR.***

II. Fragmentation in the EU Member States related to data transfers

The European Data Protection Board (EDPB) and national data protection authorities (DPAs) should play an important role in ensuring that the GDPR is interpreted and enforced in a harmonized manner across the EU Member States. This is important for individuals to benefit from a coherent application of data subjects' rights and redress mechanisms, and for companies to have the guidance they need to reach compliance while being able to tailor their compliance programs to their specific situation and needs.

However, a harmonized privacy regime across the EU is not always a reality due to **different and sometimes conflicting views of the DPAs** or due to the **use of specific derogation clauses in the GDPR**, for example:

- Several DPAs have exhibited a tendency to question the applicability of the **risk-based approach**, particularly concerning **Chapter V** of the GDPR on transfers of personal data to third countries or international organizations. The GDA perceives a risk in the overly restrictive interpretation of the Schrems II judgment, suggesting that the risk-based approach no longer applies to data transfers under Chapter V of the GDPR. This creates a dangerous gap between the risk-based approach, a core principle of the GDPR, and its practical interpretation by the DPAs and the EDPB.

- National DPAs approach towards **IP addresses** differ in Member States, which can affect whether IP addresses are subject to the GDPR's data transfer requirements. In the case C-582/14 Breyer v. Bundesrepublik Deutschland[8], the European Court of Justice considered that IP addresses are not always "personal data" subject to the GDPR. The court explained that dynamic IP addresses constituted personal data only if the processor of the IP address could link the IP addresses to an individual. Unfortunately, several DPAs have rejected the relative approach explained in the before-mentioned judgment and believed that IP address should always be considered personal data (e.g. decisions of Austria's DPA in December 2021, France's DPA in February 2022, Italy's DPA in June 2022). Only a very few DPAs followed the approach of the Breyer case (e.g. decision of Spain's DPA in December 2022). Therefore, guidelines (if not legal clarification of the GDPR) that IP addresses should not be considered personal data when they cannot be linked by an entity to a real person would help to address this problem. If this issue is not clarified, IP addresses in some Member States would continue being considered personal data in all cases, which would make IP address a subject to the GDPR's data transfer restrictions. This would be very problematic since both the functioning of the global Internet and advanced cybersecurity services depend on the

[7] Information Sharing and Analysis Centers (ISACs) — ENISA (europa.eu)

[8] 62014CJ0582 (europa.eu)

cross-border processing of IP addresses. In addition, this could lead to further fragmented application of these GDPR provisions.[9]

In light of the above, fragmentation creates unequal interpretation of the GDPR across Member States. This significantly affects global companies operating in multiple Member States as they need to introduce amendments to their business services to ensure they meet any additional or differentiating national requirements even to satisfy EU obligations. *Therefore, not only should the EDPB issue more targeted and centralized guidance that promotes harmonized application of the GDPR's obligations, but the DPAs should also be granted sufficient human recourses to effectively advice and guide businesses, as well as provide timely responses to inquiries.*

Closing Remark

The GDA thanks the European Commission for providing the opportunity to comment on these important matters. For further information please do not hesitate to contact Irma Gudziunaite, Director, Policy – EMEA, irmag@bsa.org.

[9] An additional cross-border data related concern regarding IP addresses and trademark protection is the lack of access to vital "Whois data" (data about who is the actual registrant behind a particular generic top level domain name). Lack of "Whois data" may correlate to a dramatic increase in cybercrime, including phishing and malware, cybersquatting, and other online frauds – activities that can result in security breaches or acts that compromise personal data protection for EU data subjects – in foreign markets. As part of the GDPR review, we encourage the Commission to clarify that Article 6 of the GDPR recognizes that there is a lawful basis for third party business owners to access "Whois data" in order to enforce their trademarks and protect the public from fraud and abuse.