Data Transfers Under the EU Data Act

This Global Data Alliance (GDA) position paper addresses the data transfer provisions (article 27) of the European Union *Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data* ("Data Act").

Background

The GDA is a cross-industry coalition of companies that are committed to high standards of data privacy and security and that rely on the ability to transfer data responsibly around the world. Cross-border data transfers power innovation and growth across the globe and all sectors of the economy,[1] with approximately 75 percent of the value of data transfers accruing to the manufacturing, logistics, agricultural and other sectors.[2] Data transfers also promote shared economic prosperity, benefitting workers and companies of all sizes.[3] Finally, numerous economic studies and surveys confirm the importance of data transfers to the EU specifically.[4]

From a technical perspective, the seamless and responsible transfer of data across transnational IT networks enables the deployment of modern and emerging technologies and services that underpin the economy. This includes technologies and services enabled by data transfers, such as AI-related data analytics and machine learning technologies, as well as cloud computing, blockchain, and new privacy-enhancing technologies. These technologies and services, accessed across transnational IT networks, support many important economic activities and priorities, including remote work and virtual collaboration, distance education, cybersecurity, fraud monitoring and prevention, anti-money laundering, investigation of dangerous counterfeit products, and a broad range of other activities relating to the protection of health, privacy, security, and intellectual property.

1) Article 27.1

Article 27, paragraph 1 of the draft Proposal provides as follows:

> "Providers of data processing services shall take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3".

Restated, Article 27 allows cross-border transfers of non-personal data from a data processor in the EU to another jurisdiction, and allows access to such data, provided that the processor takes the specified measures to prevent "international transfer or government access" where "such transfer or access would create a conflict with EU or member state law". Importantly, the explanatory memorandum also underscores that "the Regulation complies with the Union's international commitments in the WTO and in bilateral trade agreements."

The GDA understands that Article 27.1 would prevent cross-border transfer and access relating to non-personal data in specific cases where another EU law or EU member state law expressly prohibits such transfer or access. To the extent that Article 27.1 operates in this manner, it should avoid transfer restrictions that are greater than necessary and that could unduly impede the EU's international connectivity and commerce with third countries.

Ambiguity regarding the circumstances in which a "conflict" may arise with EU law or Member State law could invite problematic legislative interpretations. To mitigate interpretative challenges for EU judicial and administrative authorities, we would recommend to clarify that Article 27.1 refers to conflicts with EU laws

or EU member state laws that expressly prohibit data transfer or access.[5] Such legislative clarification could help forestall alternative interpretations that data transfer or access must be blocked on the basis of a much wider and less defined scope of potential "conflicts" with EU law or member state law. Indeed, if data transfer or access were halted in this unpredictable and broad manner, it could raise questions regarding the EU's compliance with its international obligations[6] and impede the future ability of EU and foreign entities to engage in cross-border commerce, R&D, and other activities.[7]

The GDA strongly supports the EU's affirmation of compliance with its existing international obligations. Consistent with those obligation, any restrictions on such transfers should be limited to what is strictly necessary to serve a legitimate public interest, be limited to the least trade-restrictive option available, not be imposed on a specific sector, and not undermine obligations to permit the cross-border provision of computing services.

2) **Article 27.2 – 27.5**

The requirements of paragraphs 2 to 5 appear tailored in a manner that create safeguards but allows, for instance, law enforcement access with sufficient due process considerations. It may be helpful to clarify the drafting of Article 27 §2 to 5 to ensure that the provisions operate in this manner. Such drafting clarifications will help ensure predictability and legal clarity, including on how the rules are going to be enforced, as well as to what will be the criteria to determine whether the measures taken comply with the law.

As drafted, some of these provisions could be read to imply that third-country law enforcement requests for data (or indeed requests from other third-country authorities) pose risks to EU organizations' IP rights in their non-personal data. The GDA is unaware of any evidence to support this interpretation. Moreover, it is unlikely that law enforcement demands for non-personal data will infringe upon fundamental rights set out in the Charter. Lastly, as regards government data access requests, B2B processors and companies (like most GDA members) that handle non-personal data for industrial manufacturing, R&D, or other enterprise purposes receive very limited – if any – data access requests given the nature of the data and services at issue. Absent such risks, the rationale for the Commission's data transfer restrictions for non-personal data are difficult to discern. Therefore, we would urge that any policy options related to government access to non-personal data issues in the international sphere should ensure a level-playing field, be proportionate to the risks, and be non-discriminatory.

Moreover, given that the stated rationale for introducing these requirements is to protect non-personal data of sensitive commercial, national security or defense value, the broad application of these provisions to all non-personal data seems overbroad and heavy-handed, particularly in light of the significant disruption to EU and foreign manufacturers and producers across all sectors of the economy.

The impact for business and global commerce on these provisions is likely to be significant. While a request for non-personal data is rare, the concern is that cloud service customers and regulators are going to be focused on whether the cloud service provider could theoretically be subject to a legislative instrument that does not meet the standards of Article 27 rather than whether non-personal data is the subject of requests actually presents a risk in practice. This could mean that deidentification, aggregation, or anonymization data are no longer seen as sufficient to protect dataregardless of the actual sensitivity of data in question. An additional point relating to the requirement to be transparent about any requests that are received (Article 27(5)) requires the provider to inform the data holder prior to disclosure. We are certain that the Commission would wish to avoid imposing rules with regard to foreign authorities that authorities in the EU could not themselves comply with. Indeed, if a third country were to adopt similar measures than those contemplated in the draft proposal, it is worth asking whether cloud service providers would be free to notify users (as contemplated in Recital 77 of the Draft proposal) in that country of any data access demands they had received from EU Member State authorities.

Moreover, the Commission's definition of the 'data holder' creates confusion, notably with regards the B2B and B2G data access and sharing, as it seems based on the false premise that technical design of a related service induces control on the product generated data.

Indeed, cloud service providers have customers that are generally businesses that own and control the data. In the context of cloud services, for example, business customers are provided assurances, both contractually and technically, that they own and control their data. Therefore, BSA members (cloud service providers), if qualified as "data holders" under the present Draft Proposal, would then be required to share data they may not have access to or are prohibited from viewing by contractual obligations with the actual controller of the data, their business customer, which owns and controls them. In case of complex datasets which could include third-party data (such as customer's providers, sub-contractors, etc.) and for which there is no direct contractual relation with the related service provider, it is even more problematic for them to be put in such a position. Moreover, this obligation may also be inconsistent with the role of processors under GDPR, because requiring processor to identify data sets to be shared and the parties with which they should be shared may constitute determinations about the "purpose and means of processing," which are left to controllers under GDPR. Therefore, especially in the context of article 27, it would be more appropriate to refer to the business customer of the data processing service provider to qualify as "data holder".

---

[1] *See e.g.,* Global Data Alliance, *Creating Jobs and Trust in Every Sector of the Economy* (2020); Global Data Alliance, *Cross-Border Data Transfers Across Sectors* (2022).
[2] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020).
[3] Need a data transfers and SMEs paper.
[4] *See e.g., Global Industry Statement in Support of a New Trans-Atlantic Data Privacy Framework* (2022).
[5] Because we understand Article 27.1 to relate to other EU or EU member state measures that already expressly prohibit data transfers, we do not understand Article 27.1 to impose a *new* obligation to prevent cross-border data transfers or access. It would be useful to clarify that Article 27 is reaffirms *existing* obligations to prevent cross-border data transfers or access, and does not create a new obligation to this effect.
[6] If Article 27.1 were applied in a manner that prohibited data transfer or access on the basis of a broad and undefined scope of potential conflicts with EU law, it could raise questions regarding compliance with the EU's transparency-related international obligations. *See e.g.,* WTO Reference Paper on Domestic Services Regulation, Art. 14 (Members shall publish "documents that provide sufficient details about such a possible new law or regulation to allow interested persons and other Members to assess whether and how their interests might be significantly affected"); General Agreement on Trade and Tariffs, Article X:1; General Agreement on Trade in Services, Article III; Trade Facilitation Agreement, Article 1. More detailed transparency obligations arise in the EU's various free trade agreements. *See e.g.,* EU-UK Trade and Cooperation Agreement, Title X. Likewise, such an interpretation could raise questions regarding compliance with commitments to permit (under the General Agreement on Trade in Services) the cross-border provision of computing services, such as cloud services, that depend upon the ability to transfer (personal and non-personal) data across borders. Article 27 mandates that such transfers be prevented, directly contradicting the EU's obligation to permit the cross-border provision of computing services. The exceptions in GATS Article XIV permitting derogations for measures "necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement" do not permit a broad override of a WTO Member's international obligations. See e.g., *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Appellate Body Report, DS363 (2010).
[7] If a court or administrative authority interpreted Article 27.1 to require that data transfers be prohibited on the basis of potential – but unspecified – "conflicts" with any other EU law and EU member state law, significant challenges could arise in the application of the Data Act. Without greater clarity regarding the operation of this provision – i.e., what constitutes a "conflict" – judicial or administrative enforcement of this provision could lack predictability, which could impede the ability of EU and foreign enterprises to plan their commercial, R&D, or other activities. For example, would differing legal requirements (e.g., regulatory requirements for product safety or testing; different technical standards in manufacturing processes, etc.) potentially give rise to such a conflict. While it appears that the legislation does not intend to require the prevention of data transfers in these circumstances, the drafting of Article 27.1 could be clarified in this regard.