BSA COMMENTS TO THE EUROPEAN DATA PROTECTION BOARD'S GUIDELINES 02/2024 ON ARTICLE 48 GDPR

BSA | Business Software Alliance ("BSA"), the leading advocate for the global software industry, welcomes the opportunity to provide feedback on the European Data Protection Board's Recommendations 02/2024 on Article 48 GDPR (the "Guidelines").

BSA members are enterprise software companies that create the technology products and services that other businesses use. For example, BSA members provide business-to-business tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and workplace collaboration software. Businesses entrust some of their most sensitive information – including personal data – with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations.

BSA supports the aim of the Guidelines to provide practical recommendations for controllers and processors in the EU that may receive requests from third-country authorities to disclose or transfer personal data. Public authorities increasingly send requests for data directly to companies. As the latest SIRIUS report (a project co-implemented by Eurojust and Europol) highlights, EU law enforcement authorities primarily use direct requests under voluntary cooperation to acquire electronic data. This trend is likely to grow with the implementation of the EU e-Evidence Regulation. It is, therefore, our understanding that third-country authorities may similarly find direct access requests to EU companies increasingly appealing.

While Article 48 GDPR shapes the enforceability and recognition of direct requests from non-EU authorities, it does not render such requests illegal, limit them to a single legal ground for transfer, or exclude any legal basis for such transfers.

Accordingly, BSA submits the following recommendations to be addressed in the final version of the Guidelines.

1. **The Guidelines should clarify how Article 48 interacts with relevant Chapter V transfer tools, such as adequacy decisions and Binding Corporate Rules (BCRs).**

While the Guidelines acknowledge that the requirements of Article 48 GDPR for an international agreement are "without prejudice to other grounds for transfers under this Chapter," they primarily discuss transfer possibilities under Article 46 GDPR (transfers subject to appropriate safeguards) and Article 49 GDPR (derogations for specific situations). Unfortunately, the Guidelines lack a meaningful reference to adequacy decisions under Article 45 GDPR, Binding Corporate Rules (BCRs) under Article 47 GDPR, Codes of Conduct pursuant to Article 40 GDPR, as well as sufficient elaboration regarding transfers subject to additional safeguards under Article 46 GDPR.

Adequacy decisions are a cornerstone of the GDPR's data transfer framework and provide robust assurances of compliance with EU data protection standards. BSA believes that the final EDPB guidance should more explicitly elaborate on Article 45 GDPR as a legal ground for data transfers outside the EU. **Therefore, in the final Guidelines, the EDPB should further specify that adequacy decisions can be relied upon as a valid basis to transfer data outside EU, with a special attention to the third country-headquartered companies with a presence in the EU and EU-headquartered companies with a presence in the third country.** In addition, the Guidelines would benefit of a mention of the European Commission's landmark adequacy decision of 10 July 2023 regarding the EU-US Data Privacy Framework (DPF). This adequacy decision is significant and worth the attention, given the practical implications for companies relying on the DPF to facilitate transatlantic data flows.

Additionally, in practice, third country-headquartered companies often receive data access requests directly from third country authorities, even when the data is physically stored outside the third country. The same applies to EU companies with a relevant third country entity or presence. For example, US-headquartered companies would receive data access requests directly from the US Department of Justice, even when the data is physically stored in the EU. Hence, the relevant data flows would take place between an EU entity and a third-country entity of one company. Therefore, **the final Guidelines should address the use of various data transfer tools, including BCRs, adequacy decisions, Codes of Conduct, and others.**

2. **The Guidelines should recognize legitimate interest as a valid legal basis for transfers in response to direct requests from third-country authorities.**

While the EDPB recognizes that a controller may sometimes have a legitimate interest in complying with a request from a non-EU authority, it nonetheless questions the possibility of relying on Article 6(1)(f) GDPR (legitimate interests) as a legal basis for such transfers. This position is motivated by the CJEU's case law in Meta Platforms Ireland Limited v. Bundeskartellamt (Case C-252/21) and the EDPB's 2019 initial legal

assessment of the US CLOUD Act. BSA is not supportive of this position and doubts the underlying reasoning in the Guidelines.

Firstly, the Meta Platforms judgment primarily concerns large-scale, indiscriminate processing of personal data to preemptively respond to potential future law enforcement requests. This scenario significantly differs from the context of responding to specific, legally binding requests from non-EU authorities on a case-by-case basis. In the same judgment, the CJEU explicitly acknowledges the legitimacy of responding to legally binding requests under appropriate conditions. This recognition aligns with the fundamental GDPR principle of balancing interests and suggests that such responses could fall within the scope of Article 6(1)(f) GDPR.

Secondly, the Guidelines reference the EDPB's 2019 initial legal assessment of the US CLOUD Act. While the 2019 document highlights challenges in assessing applicable standards, procedural guarantees, and proportionality principles in the absence of an international agreement, it does not categorically exclude the use of a legitimate interest. Instead, it points to the complexity of such assessments in the absence of a robust legal framework. The Commission's adequacy decision of 10 July 2023 regarding the EU-US DPF directly addresses many of the concerns raised in the 2019 legal assessment. Specifically, the adequacy decision carefully evaluates due process protections, procedural safeguards, and proportionality principles in US criminal procedure law (paragraphs 90-118). **BSA considers that these elements provide a solid foundation for relying on legitimate interests as a legal basis, especially, for responding to requests from US authorities, or at least for intra-company transfers in view of answering such requests.** BSA, therefore, suggests that the final EDPB guidance reassess the use of Article 6(1)(f) GDPR as a basis for complying with legally binding requests, especially when robust safeguards are in place. This is all the more desirable as the last sub-paragraph of Article 49(1) explicitly shows that the legislator intended to allow certain data transfers based on the controller's "compelling legitimate interests," even when such transfers cannot rely on Articles 45, 46, or the derogations in Article 49(1)(a) to (g).

Addressing these points would provide clearer and more balanced guidance for companies navigating the complexities of international data transfers and ensuring compliance with both GDPR and relevant third-country legal obligations.

BSA and its members appreciate the opportunity to comment on the Guidelines and stand ready to further assist the EDPB as it finalizes the Guidelines.

For more information, please contact Irma Gudziunaite, Director, Policy – EMEA at BSA, via email at irmag@bsa.org.