ITI Promoting Innovation Worldwide

ITI Comments to the European Data Protection Board (EDPB) Guidelines 02/2024 on Article 48 GDPR

27 January 2025

The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader for the global information and communication technology (ICT) industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI member companies represent the breadth of the technology ecosystem, including semiconductor and computer hardware and software companies, network equipment manufacturers and suppliers, cybersecurity providers, and leading Internet services and consumer technology companies.

Privacy and trust are central to our member companies' businesses and global operations. Together with our members, ITI works with governments, regulators, and stakeholders around the world to strengthen and align approaches towards data protection and privacy that safeguard individual rights and promote innovation.

I. Introduction

ITI appreciates the opportunity to provide comments to the proposed European Data Protection Board (EDPB) Guidelines 02/2024 on Article 48 GDPR (the "Guidelines"). These Guidelines offer important clarifications on the conditions under which controllers and processors may respond to requests from third-country authorities and outline practical steps to ensure compliance with Article 48.

However, ITI is concerned that the Guidelines take an overly restrictive stance on data transfers to non-EU authorities for law enforcement purposes, particularly regarding the application of legal bases under Article 6 GDPR, such as consent and legitimate interest, in cases where no legal obligation arises from an international agreement. Additionally, the Guidelines should provide clearer guidance on how processors should respond to direct requests from third-country authorities, especially in cases where criminal law obligations prevent notifying the controller. Furthermore, ITI notes that the Guidelines underemphasize Article 45 GDPR as a potential legal ground for cross-border data transfers.

Finally, ITI emphasizes that while Article 48 can impact the enforceability and recognition of requests from non-EU authorities, such requests are not unlawful per se. Instead, it establishes critical safeguards to ensure such requests comply with EU data protection principles. Additionally, it is important to recognize that EU Member States frequently issue similar requests to U.S.-based companies, relying on various mechanisms[1]. These practices are expected to likely increase when the

[1] https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2024

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

e-Evidence regulation enters into force. Such considerations call for a balanced and practical approach in the Guidelines. An overly restrictive stance risks creating unnecessary legal uncertainty and could undermine cooperation between EU and non-EU jurisdictions, even where robust safeguards exist.

II. Specific concerns relating to the guidance on legal bases for processing in case no legal obligation arises from an international agreement

a. Use of consent as a legal basis (Article 6 (1) (a))

The Guidelines (paragraph 21) state that the "*use of consent will be* usually *inappropriate in certain areas, especially, if the processing of the data is related to the exercise of authoritative powers*". ITI acknowledges that consent may not be appropriate in contexts involving compulsory powers. That said, we caution against broadly categorizing consent as "usually inappropriate". In certain contexts, such as business-to-business (B2B) relationships, informed consent can serve as a viable legal basis. For instance, when a cloud service provider subject to a non-EU authority request redirects such requests to large enterprise customers, informed consent can work as a proper legal basis. In practice, many large cloud service providers explicitly outline this process in their General Terms and Conditions. ITI recommends that the Guidelines recognize such scenarios where consent functions as an appropriate legal basis, ensuring that businesses retain practical mechanisms for compliance.

b. Use of legitimate interest as a legal basis (Article 6 (1) (f))

Paragraphs 25-26 of the Guidelines find that legitimate interest to comply with a request from a non-EU authority can only be used in exceptional circumstances. The Guidelines also state that controllers "*may sometimes have a legitimate interest to comply with a request from a non-EU authority*". However, they restrict the possibility to rely on article 6 (1) f), in view of the CJEU's case 252/21 Meta Platforms Inc and Others v Bundeskartellamt[2] and the EDPB's 2019 initial legal assessment of the impact of the U.S. Cloud Act[3]. Such framing is overly restrictive.

Firstly, the CJEU's judgment in Meta Platforms (Case C-252/21) addressed large-scale, anticipatory data collection rather than case by case responses to individual legal requests of authorities and should not be applied as a blanket precedent for all scenarios. In fact, the CJEU in the same case recognized the legitimacy of responding to binding legal requests, underscoring the importance of context.

Furthermore, the Guidelines only partially refer to its 2019 legal assessment of the Cloud Act which did not exclude a legitimate interest balancing test per se, but instead noted challenges in the absence of an international agreement. These challenges included, for instance, assessing applicable

[2] Judgment of the Court (Grand Chamber) of 4 July 2023, Meta Platforms Inc and Others v Bundeskartellamt, Case C-252/21, para. 124 and 132.

[3] https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en

standards and procedural guarantees in the U.S., the data applicable protection and proportionality principles, and the right to an effective remedy. It is crucial to note, that meanwhile those elements have been scrutinized in the Commission's adequacy decision of 10 July 2023 regarding the EU-U.S. Data Protection Framework (DPF). The adequacy decision, particularly in paragraphs 90-118, provides a comprehensive assessment of due process protections and other safeguards under U.S. criminal procedure law. This is therefore relevant background for the EDPB's current analysis of whether legitimate interests can constitute a valid legal basis for compliance with requests from U.S., or in any event for intra-company transfers in view of answering such requests. We recommend that the EDPB further reflects these considerations in the final guidance to ensure a less restrictive approach.

III. Lack of clearer reference to article 45

The Guidelines, in section 5.2 "Compliance with Chapter V GDPR" and particularly in paragraphs 30-31, extensively reference Article 46(2) GDPR but do not specifically and comprehensively discuss the use of Article 45 GDPR as a possible legal ground for such transfers, nor do they address the European Commission's landmark adequacy decision of 10 July 2023 regarding the EU-U.S. Data Privacy Framework (DPF). In the same vein, section 32 of the draft guidance, acknowledges that Article 48 GDPR's requirements for an international agreement are "without prejudice to other grounds for transfers under this chapter." However, it only references Article 49 GDPR and makes no mention of Article 45 GDPR.

In this respect, the European Commission has also clarified, in its past submission to the U.S. Supreme Court[4] (see p. 14), that Article 48 GDPR does not provide an absolute ban. Particularly, the Commission qualifies transfers under MLATS as one ground of transfer (even if a preferred one) among potentially applicable other grounds for transfer, such as article 45 GDPR.

This is especially relevant for U.S. headquartered companies, where access requests from the U.S. are directly requested to the U.S. entity even if the data is located outside the U.S. The same dynamic will likely apply to EU companies with a U.S. presence, where intra-company transfers between EU and U.S. entities are a common occurrence. Those scenarios reinforce the importance of further clarifying that Article 45 is a key legal ground for such transfers. To ensure the Guidelines are practical, we strongly recommend that the final EDPB Guidelines more explicitly reference Article 45 GDPR as a valid and critical legal basis for cross-border data transfers and emphasize that additional safeguards under Article 46 are necessary only in the absence of an adequacy decision.

[4] https://www.supremecourt.gov/docketpdf/17/17-2/23655/20171213123137791_17-2%20ac%20european%20commission%20for%20filing.pdf