COMMENTS ON PROPOSED EDPB GUIDELINES 02/2024
(JANUARY 27, 2025)

The United States appreciates the opportunity to comment on the proposed European Data Protection Board (EDPB) Guidelines (02/2024). The United States asks that the EDPB revise the Guidelines (1) to remove any suggestion that a lawful order to a company, subject to a country's legal jurisdiction, to produce data held in another country may violate international law; and (2) to incorporate in the Guidelines language that, in an era of increasing data flows, recognizes the importance of facilitating cross-border data requests that are consistent with the rule of law.

I. The Guidelines Should Remove Any Suggestion that Data Requests Issued to a Company Subject to a Country's Jurisdiction Violate International Law.

The Guidelines state that Article 48 "protect[s] personal data from the extraterritorial application of third country laws which may be in breach of international law."[1] The statement should be clarified because it could be read to suggest that lawful third-country requests that require a company subject to that third country's jurisdiction to transfer personal data held in the EU may violate international law.[2] That suggestion is contradicted by the GDPR provisions discussed elsewhere in the Guidelines, which allow controllers and processors to comply with such orders in some circumstances. The suggestion is also inconsistent with the law and practice of the EU and Member States and the text of Europe's Convention on Cybercrime (Budapest Convention).

The Guidelines themselves clarify that the GDPR authorizes transfers of data in response to compulsory third-country data requests in several circumstances, even absent an international agreement. As the Guidelines state in the Executive Summary, "if there is no international agreement or the agreement does not provide for appropriate safeguards . . . , other grounds for transfer could apply, including the derogations in Article 49."[3] The Guidelines later explain several possible situations, even in the absence of an international agreement or where an agreement lacks the safeguards required by Article 46, in which a controller or processor may transfer data to a third country in response to a third-country data request by relying on other GDPR provisions for the processing and transfer of the data.[4]

EU law authorizes Member States to order a company to disclose data held outside of the EU. The EU's e-Evidence Regulation, 2023/1543, in Article 1(1) authorizes Member States to "order a service provider . . . to produce or preserve electronic evidence regardless of the location of data." The laws of Member States, including Belgium, Denmark, France, Ireland, and Spain,

[1] Guidelines para. 8 (quoting GDPR recital 115) (internal quotations removed).

[2] Third-country data requests subject to Article 48 are obligatory. Article 48 refers to requests from a "third country requiring a controller or processor to transfer or disclose personal data . . . ." (Emphasis added.) The proposed Guidelines reiterate at paragraph 19 that "[t]he case described in Article 48 presupposes that there is a judgement of a court or tribunal or a decision of an administrative authority of a third country that requires a controller or processor in the EU to transfer or disclose personal data." (Emphasis added.)

[4] Guidelines para. 32.

also include such authority. Consistent with EU law and the laws of these Member States, the laws of the United States likewise authorize federal judges to issue warrants to companies subject to U.S. jurisdiction that require the disclosure of data "regardless of whether such [data] is located within or outside of the United States."[5]

These national laws authorizing requests to require disclosure of data held in another jurisdiction implement obligations imposed by the Budapest Convention. Article 18(1)(a) of the Budapest Convention requires each Party to the convention to adopt national laws under which relevant authorities can compel providers in their territory to disclose electronic data in their possession or control.[6] The Explanatory Report to Article 18 specifically notes that the article covers "situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from *within* the ordering Party's territory."[7] This language requires that the person in control of the data must be within the Party's territory but does not impose a similar requirement on the location of the data that is in that person's possession or control. Article 27(a) of the recently adopted UN Convention Against Cybercrime contains the same obligations as those set forth in Article 18(1)(a) of the Budapest Convention.

Accordingly, the United States recommends clarifying the language in paragraph 8 of the Guidelines to avoid any suggestion that such compulsory requests might violate international law. That does not appear to be the view of the EDPB, based on other parts of the Guidelines, but the language could be misconstrued. The clarification is important to the discussion of the other grounds for transfer outlined in the Guidelines, which acknowledge that such transfers may be lawful without an international agreement.

II. The Guidelines Should Recognize the Importance of Cross-Border Data Requests in the Guidelines' Analysis of the Grounds for Transfers Under GDPR.

Far from breaching international law, cross-border requests for data are increasingly a necessary component of national investigations in rule-of-law countries to counter serious crime and protect public safety and security. As a European Commission report has identified, in over two-thirds of European criminal investigations in which electronic evidence is relevant, there is a need to obtain evidence from service providers based in another jurisdiction.[8] As discussed

[5] 18 U.S.C. § 2713. The United States frequently relies on this authority when responding to mutual legal assistance requests from EU Member States for data controlled by U.S. companies including where the location of the data is unknown, is frequently shifted for the company's business purposes, or is stored in multiple locations.

[6] Article 18(1)(a) of the Budapest Convention obligates each Party to "adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium."

[7] Explanatory Report to the Budapest Convention, CETS 185, paragraph 173 (emphasis added).

[8] Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in

above, to ensure that law enforcement agencies and other national authorities can obtain such data located in other jurisdictions, the EU, many Member States, the United States, and other countries have expressly authorized data requests.

The authority to obtain data relevant to an investigation has become increasingly important based on the data storage practices of large electronic communications providers. The providers frequently hold data in multiple countries, and some providers continually move data among storage facilities located in multiple countries for business purposes. And some providers may store data related to the same message in multiple data centers in multiple jurisdictions. As a result, even when investigators seek data relating to an offense in their country, from a provider subject to their jurisdiction, it may be impossible to know where the provider stores the data. Meanwhile, the provider may have access to all of that data from the investigating country.

EDPB Guidelines addressing the application of GDPR provisions that authorize companies to respond to cross-border data requests should recognize the importance of facilitating such legitimate requests for data, consistent with privacy protections. Indeed, governments from rule of law countries are actively engaged in efforts to create frameworks facilitating such requests. For example, negotiators of the Council of Europe's Second Additional Protocol to the Budapest Convention recently recognized the need for additional mechanisms for access to data, and the resulting Protocol provides new tools for enhanced cooperation and the disclosure of electronic evidence, including articles providing for direct cooperation with service providers and registrars to obtain subscriber information and domain registration information, while also providing data protection and privacy safeguards.

These efforts follow the United States's initiative in 2018 to address potential conflicts of law resulting from data requests, including those involving U.S. electronic communications service providers which, as a result of their global prevalence, are sometimes holding data relevant to other countries' investigations, by passing the CLOUD Act. The CLOUD Act authorizes the United States to conclude agreements with foreign governments to facilitate access to data held in each other's jurisdiction to counter serious crime,[9] and it also amends U.S. law to permit disclosures of data in response to a foreign government's data request based on such an agreement.[10] The European Commission and the United States are currently negotiating such an agreement to improve each side's access to data to enable more effective investigations to counter serious crime.

In addition, in the recently concluded negotiation of the UN Convention Against Cybercrime, the EU and Member States, as well as the United States, approved language in the international cooperation chapter urging parties to cooperate rather than simply to refuse to provide data when the transfer might conflict with data protection laws. Article 36 of the adopted text, while

---

criminal proceedings, SWD (2018) 118 final, p. 14. *See also* Sirius EU Electronic Evidence Situation Report 2024.

[9] 18 U.S.C. § 2523.

[10] 18 U.S.C. § 2702(b)(9).

permitting parties to refuse to provide data on data protection grounds, encourages parties to impose conditions so that a transfer of personal data in the context of international cooperation may take place. The convention further encourages parties to engage in multilateral and bilateral arrangements to allow international transfers of personal data for the purpose of investigating and prosecuting serious crime.

We recommend that the EDPB amend the Guidelines by placing its discussion of GDPR provisions governing how controllers and processors may respond to third-country data requests in the appropriate context. The Guidelines should recognize that such requests are a common and necessary aspect of modern international relations resulting from nations' efforts to enforce their domestic laws. For example, the discussion of examples of third-country data requests subject to Article 48 at paragraphs 4 and 13 of the Guidelines should recognize the ongoing efforts of the EU and other countries to facilitate such legitimate requests for data, and the importance of such efforts to enable enforcement of domestic laws. Third-country data requests should not be characterized as breaching international law, but rather as a matter to be managed through cooperation among democratic countries committed to the rule of law.