ITI Promoting Innovation Worldwide

31 January 2022

ITI Comments to the European Data Protection Board (EDPB) Guidelines 05/202 on the Interplay between the Application of Article 3 and the Provisions on International Transfers as per Chapter V of the GDPR

ITI is the global voice of the tech industry. Our 80 member companies include leading innovation companies with worldwide value chains and active through all the segments of the technology sector. Our industry shares the goal of safeguarding privacy, and together with our members, we are working with European and global institutions as well as national Data Protection Authorities (DPAs) around the world on key data protection and privacy issues, including the General Data Protection Regulation (GDPR).

ITI endorses strong protections for personal data transfers to third countries, and we are pleased to provide our input to the EDPB's *Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (hereinafter, "the Guidelines"). We appreciate the Board's efforts in drafting the document under consultation. In particular, we seek clarification on data transfers regarding the relationship between the EDPB guidelines and European Commissions' Standard Contractual Clauses (SCCs) in situations where controllers or processors are already subject to the GDPR. We further recommend making clear that the use of current SCCs are sufficient tools and there is no need to adopt an alternative contractual agreement.

Privacy and user trust are central to our member companies' businesses and global operations. Our comments below outline our desire to seek further clarification. We look forward to a constructive exchange with the EDPB on these ideas and remain at your disposal for continued discussions.

ITI General Comments

Clarify the Relationship Between the SCCs and Guidelines

The Guidelines are essential to all stakeholders in clarifying what constitutes an international transfer. In situations where controllers or processors are already subject to the GDPR, it should be clear that companies adopting the SCCs from the European Commission text published in 2021 provides sufficient basis for a transfer, and there is no need for an alternative contractual agreement. In particular, we note that paragraph 23 may imply that there are no transfer tools for a transfer of personal data to a controller subject to the GDPR in a third country, especially in cases where a conflict of laws exists between third country legislation and the GDPR, and suggest that EDPB consider developing a new set of SCCs in cases where the importer is subject to the GDPR for the given processing, to avoid confusion and concern.

The problem is that currently there is no SCC for a scenario in which a data importer is directly subject to the GDPR. According to the recent European Commission SCCs as stated in Recital 7, the SCCs may be used for such transfers only to the extent that the processing by the importer does not fall within the scope of Regulation, in other words, the SCCs are not applicable if the data importer is already subject to the GDPR. Private sector commentators have characterized this statement as a "design

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

error" since, currently, there is no other mechanism or template for data transfers available to companies in this specific scenario. In the absence of other options, most companies are updating their SCCs and applying them, even when they are also importers of data directly regulated by the GDPR. Although the Commission has identified the gap and promised an additional template for use in these specific cases, no other solution has been presented so far.

As the EDPB points out, the currently available SCCs may result in duplication of GDPR obligations. In practical and day-to-day situations, contractual duplication of statutory obligations, when safeguarding fundamental rights, are quite common and do not pose risks or issues to the interested parties. We would therefore suggest a clarification that the use of the current SCCs for these scenarios may result in sufficient compliance, thereby avoiding the implication that there is currently no viable means of compliance for this common scenario, or that the use of the current SCCs results in non-compliance.

Without clarity, it leaves business in the dark as to what they should adhere to. It is unclear to companies whether they should adhere to the Standard Contractual Clauses (SCCs) published by the European Commission or follow the EDPB guidelines. As a result, we seek clarification regarding the latest status of the EDPB guidelines, and how companies should interpret their relationship with the current SCCs.

Ensure Consistent and Accurate Terms/Terminologies

The EDPB guidelines can be improved by unifying terms. Throughout the guidance, two different terms -- "accessible" and "available" -- are used to refer to data disclosed by transmissions. However, data can be available on a server or traveling through a network, but not accessible to anyone who is not the owner of the encryption keys to decrypt the data. We suggest the EDPB unify the terminology and refer to accessible (instead of available) data for consistency and clarity. Additionally, risk assessments conducted by companies have shown that the level of risk is not the same when there is a data "transfer" compared to a data "access." For example, we notice that the guidelines state that mere access from outside the European Economic Area (EEA) would not always amount to a transfer in the meaning of Chapter V GDPR. Even if companies are keeping some data in the EEA, issues often arise in the context of providing 24/7 customer support. When a remote maintenance provider outside the EU has access to data which technically remains stored in the EU, the risk is significantly lower because there is no "actual" data transfer. In consequence, the EDPB should differentiate among these scenarios and update the terms as appropriate.

Welcome Clarity on Transfer Impact Assessment

It is not clear whether and to what extent the transfer impact assessment should involve a risk-based approach or a case-by-case rights-based approach. We would welcome clarity on what could be the characteristics of a personal data transfer/access that could be in the scope of analysis when applying a risk-based approach and case-by-case rights-based approach. We take into account the need to avoid weakening the GDPR individual rights in respect of their personal data subject matter of transfer to/access from third countries; however, enforcement of a risk-based "0-tolerance" interpretation would adversely interfere with other rights and freedoms of third parties granted by the Charter of Fundamental Rights of the EU (e.g., the freedom of information (Art. 11), the freedom to conduct a business (Art. 16) and the right to property (Art. 17)), that must be weighed in balance with an enforcement. It is our view that only a risk-based interpretation would preserve this

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

proportionality, i.e., an approach which considers that, while no personal data processing is risk-free, not every risk leads to an unjustifiable violation of the rights of individuals.

We would also welcome additional clarity on the EDPB's approach towards the onward transfers to third countries when conducting a transfer impact assessment. In particular, the EDPB recommendation could imply that the exporter should obtain information on each onward transfer (including all transfers performed in its subcontracting chain), which would render the assessment extremely lengthy and sometimes almost impossible to perform in the cases of complex projects (e.g., projects involving multiple tiers of subcontractors). To prevent the risk of unnecessarily impeding business operations with endless data transfer analysis and contracts that would create needless obstacles to data flows and economic cooperation, our proposed approach is that the exporter should only acknowledge (and eventually map) relevant transfers in the transfer impact assessment documentation, to their best of their knowledge at the time when they are conducting the transfer. At the same time, the exporter should obtain from all its subcontractors contractual commitments and sufficient guarantees that the GDPR requirements will be observed throughout the entire personal data transfer chain until the final recipient of such data. In the case of exporters' processors, this could be accomplished by including relevant provisions in the data processing agreements to be concluded under Art. 28 of GDPR.

ITI Specific Comments

Below, we offer three specific recommendations to improve the text:

- **Paragraph 12**
  First, the EDPB's current proposed criteria to qualify a processing as a transfer of personal data to a third country or an international organization (hereinafter a "third country") does not provide detailed information regarding the transfer cases where Art. 3 recitals (2) and (3) of GDPR are applicable (where GDPR has an extraterritorial effect). While we welcome the Guidelines' general reference to the criteria of the exporter (controller or processor) being subject to the GDPR for the given processing, we believe there is a need to add detailed explanations and sample cases/scenarios so that the interplay between Art. 3 recitals (2) and (3) of GDPR and Art. 44 of GDPR can be comprehensively understood by all relevant stakeholders.

  Additionally, We would welcome the addition of more details and sample scenarios in Section 2.2 paragraph 12, specifically in cases where there are no data transfers if individuals disclose their own personal data directly on their own initiative, or when the personal data is collected from the individuals at the initiative of a non-EEA controller or processor (passively, thus not at the initiative of the individuals) or by the individuals acting as controllers/processors under Art. 4(7) and (8) of GDPR(e.g., as self-employed persons).

- **Example 3: Processor in the EU sends data back to its controller in a third country**
  Second, we would welcome clarifications from EDPB to stress that only data that hasn't been previously accessible to XYZ Inc. can be "disclosed" by ABC to XYZ. Semantically a "disclosure of data" implies that the recipient of the disclosure does not or did not already have that data. We believe that this lack of clarity regarding what constitutes a disclosure in such circumstances is a fundamental reason underlying the second criterion proposed in the Guidelines. Additionally,

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

the first sentence of Example 3 should be changed into "XYZ Inc., a controller established outside the EU, whose processing of personal data of its employees/customers is not subject to the GDPR, sends that personal data to the processor ABC Ltd., which has an establishment in the EU, for processing on behalf of XYZ." The reasons we suggest making this change are that (a) the GDPR could apply even without an EU establishment of the controller, (b) residency of data subjects is irrelevant under the GDPR, and (c) location of the data processing activity is irrelevant under the GDPR.

Including this suggested change, "Example 3: Processor in the EU sends data back to its controller in a third country" would read in whole as follows:

"XYZ Inc., a controller established outside the EU whose processing of personal data of its employees/customers is not subject to the GDPR, sends that personal data to the processor ABC Ltd., which has an establishment in the EU. ABC transmits that data plus additional personal data processed by ABC on behalf of XYZ back to XYZ. The processing performed by ABC, the processor, is covered by the GDPR for processor specific obligations pursuant to Article 3(1), since ABC is established in the EU. XYZ is a controller in a third country. Any data added by ABC is a disclosure of data from ABC to XYZ and is regarded as a transfer of personal data and therefore Chapter V applies to such data. Data that had been previously sent by XYZ to ABC and is merely sent back, cannot be considered as disclosed to XYZ, given that the data already had been in XYZ's possession and therefore is not regarded as transferred."

- **Paragraph 17**

Third, this section states that *"the controller is accountable for its processing activities, regardless of where they take place, and must comply with the GDPR, including Article 24 ("Responsibility of the controller"), 32 ("Security of processing"), 33 ("Notification of a personal data breach"), 35 ("Data Protection Impact Assessment"), 48 ("Transfers or disclosures not authorised by Union law"), etc. Following from its obligation to implement technical and organisational measures taking into account, inter alia, the risks with respect to the processing under Article 32 of the GDPR, a controller may very well conclude that extensive security measures are needed – or even that it would not be lawful – to conduct or proceed with a specific processing operation in a third country although there is no "transfer" situation".*

We note the Guidelines suggest that Art. 48 of GDPR is applicable when a certain data flow may not qualify as a "transfer" to a third country in accordance with Chapter V of GDPR. However, Art. 48 of GDPR prohibits the disclosure of personal data to a foreign authority unless the parties can rely on an international agreement such as a mutual assistance treaty and a personal data transfer is intended, while in this situation there is no personal data transfer envisaged.

While we agree that because there is no disclosure, there is no transfer in situations where the sender and the recipient are the same entity, this paragraph goes beyond that to suggest that a controller or processor may conclude that extensive security measures are needed – or even that it would not be lawful – to conduct or proceed with a specific processing operation in a third country irrespective of whether it involves a transfer. This suggestion will introduce tremendous confusion to the challenging situations companies are already facing, particularly companies with less resources, and would undermine the validity and importance of the adequacy status of the fifteen third countries currently being relied upon for a vast number of these "non-transfers."

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

For example, based on this suggestion in the draft Guidelines, all controllers who have been "transferring" EU data to themselves in Canada, Switzerland or Japan (e.g. companies in those countries importing data to themselves or EU companies exporting data to themselves in those countries), would be left in doubt as to whether they could continue to rely on the adequacy status of their respective countries.

It is also not clear whether the EDPB's recommendation in this situation is that the controller should perform a separate specific assessment (similar to a data protection impact assessment or to a transfer impact assessment) of the above-mentioned risks in order to decide if the processing should proceed. It would be helpful for EDPB to clarify within which conditions -- including if there are any necessary, appropriate, and available supplementary measures to additionally protect the personal data involved, or an assessment of the above-mentioned risks -- would be included in controller's endeavors to observe its accountability obligations under GDPR.

We therefore proposed deleting the above quoted language and replacing the language in paragraph 17 as follows:

"Although a certain data flow may not qualify as a "transfer" to a third country in accordance with Chapter V of the GDPR, including example 5, such processing can still be associated with risks, for example due to conflicting national laws or government access in a third country as well as difficulties to enforce and obtain redress against entities outside the EU."

Alternatively, if the EDPB decides to maintain the Paragraph 17 language, it should be augmented with a clarification that the adequacy of a third country and safeguards similar as those enumerated in Art 46 of the GDPR are a relevant factor even if there is no "transfer" situation. The EDPB should also clarify that the risk-based approach and article 32 of the GDPR should be interpreted to mean technical and organizational measures, but not necessarily the Supplementary Measures outlined by the EDPB's recommendations when applying SCCs for an international data transfer.

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