efpia European Federation of Pharmaceutical Industries and Associations

IPMPC International Pharmaceutical & Medical Device Privacy Consortium

21 December 2020

Dr. Andrea Jelinek, Chair
European Data Protection Board
Rue Wiertz 60, B-1047 Brussels

Re: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Dear Dr. Jelinek,

The European Federation of Pharmaceutical Industries and Associations (EFPIA) and the International Pharmaceutical & Medical Device Privacy Consortium (IPMPC) welcome the possibility to provide comments in response to this Consultation. EFPIA represents the biopharmaceutical industry operating in Europe. Through its direct membership of 36 national associations, 39 leading pharmaceutical companies and a growing number of small and medium-sized enterprises (SMEs), EFPIA's mission is to create a collaborative environment that enables its members to innovate, discover, develop and deliver new therapies and vaccines for people across Europe, as well as contribute to the European economy. The IPMPC is comprised of chief privacy officers and other data privacy and security professionals from a number of research-based, global pharmaceutical companies and medical device manufacturers. The IPMPC strives to be a leading voice in the global pharmaceutical and medical device industries to advance innovative privacy solutions to protect patients, enhance healthcare, and support business enablement.[1]

The ability to transfer personal data across borders is critical to healthcare innovation and delivery. The right of access to preventive health care and the right to benefit from medical treatment is a fundamental right recognised in the EU Charter of Fundamental Rights, and any interference with this right must be based only on other competing concrete risks. Pharmaceutical and medical device companies have implemented extensive technical and administrative safeguards to protect the privacy of patients, their caregivers, and the researchers who work tirelessly to develop new treatments, and these safeguards apply both to data processing that occurs within the European Union as well as to data processed in other jurisdictions.

The EDPB's *Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* puts forward a number of examples of supplementary measures that organizations might consider when relying upon transfer tools under GDPR Art. 46. In many cases, however, the document appears to dismiss these measures as insufficiently effective. In some cases, the document fails to

[1] More information about the IPMPC is available at www.ipmpc.org. This filing reflects the position of the IPMPC as an organization and should not be construed to reflect the positions of any individual member.

fully appreciate how certain measures can provide a level of data protection that is of 'essential equivalence' to that guaranteed under EU law.

A. An assessment of public authorities' access to data transferred from the EU should take into account objective factors relevant to understanding the risk of such access.

An assessment of public authorities' access to data transferred from the EU should focus on the realistic risk of such access and consequences for data subjects, not simply on some highly theoretical possibility. In many cases, laws authorizing public authorities to request access to data from private organizations are unclear in their scope of application. Interpretation of these laws necessitates looking to objective facts outside the text of the law - including historical practices, policy statements, and precedent. This is integral to arriving at an objective understanding of whether public authorities will request access to data.[2] A thorough analysis should consider factors such as the types of entities from whom public authorities are authorized to request access, the purposes for which public authorities are authorized to request access, the data categories relevant and of interest to such public authorities, and whether any transferred data would be responsive to such requests. This analysis can be informed by examination of whether foreign public authorities have ever previously requested access to a company's data or to data of similarly situated companies in the same industry. We note that the European Commission has suggested a similar, contextual approach to this assessment in its consultation on proposed new standard contractual clauses for data transfers outside of the EU, and we are supportive of the Commission's approach.[3]

While theoretical possibilities should not be ignored in such an analysis, there is nothing in the GDPR or in the judgment of the European Court of Justice in *Schrems II* that requires data exporters and importers to focus solely on theoretical possibilities to the exclusion of actual historical practices. If an organization does not transfer data from the EU that would reasonably be requested by foreign public authorities based on consideration of objective factors, it is reasonable for an organization to conclude that GDPR Article 46 transfer tools provide a level of data protection that is essentially equivalent to that found in the EU.

B. The application of GDPR Article 49 (a) through (f) derogations depends on whether the conditions specified therein apply, not on whether the transfers are of a repetitive nature.

GDPR Article 49 lists a number of 'specific situations' in which transfers of personal data are permissible despite the absence of an adequacy decision under Article 45(3) or of appropriate safeguards under Article 46. These specific situations are laid out in Art. 49(1), subparagraph 1, points (a) through (g), and then there is a further derogation in subparagraph 2 that applies to transfers based on compelling legitimate interests '[w]here a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable,' provided that certain conditions are met. Among these conditions is that the transfer is not repetitive. Notwithstanding that the text of Art. 49(1) is clear that the non-repetitive condition applies only to reliance on the compelling legitimate interests derogation, the document describes this as a condition that applies to points (a) through (g) as well. ('Only in some cases of occasional and non-repetitive transfers you may

---

[2] We note that the EDPB itself relies on evidence of past practice in Use Case 5.

[3] European Commission, proposed Implementing Decision on standard contractual clauses for the transfer of personal data to third countries, at para. 20 ('The parties should take into account . . . any relevant practical experience indicating the existence or absence of prior instances of requests for disclosure from public authorities received by the data importer for the type of data transferred. . . .')

be able to rely on one of the derogations provided for in Article 49 GDPR, if you meet the conditions.' Executive Summary at p. 2.)

The EDPB's overly restrictive interpretation of the Article 49 derogations does not align with the lawmakers' determinations of how to most appropriately balance data protection rights with other important rights and interests. The fact that the wording of Article 49(1) only includes 'not repetitive' as a condition of the compelling legitimate interests derogation reflects lawmakers' determination that this condition should not apply more generally. Recital 111, which the EDPB has previously pointed to as necessitating a restrictive reading of the Article 49 derogations[4], does not support this restrictive reading. Recital 111 uses the term 'occasional' only in relation to transfers that are necessary for contractual or legal claims, situations which one would anticipate arising only on an occasional basis.[5] The more expansive application of the 'occasional' and 'non-repetitive' conditions in the *Recommendations 01/2020* is unsupported by the legal text.

We urge the EDPB to reassess its prior guidance concerning the conditions for use of the Article 49 derogations in light of the outcomes of the *Schrems II* case. The Board's 2018 guidance was based on a presumption of the availability of the Article 46 safeguards as a means to provide a legally sufficient level of data protection in most ordinary circumstances. To the extent the Article 46 safeguards are no longer sufficient in combination with other reasonably implementable technical, contractual, and organisational measures to allow multinational companies to continue to perform necessary business functions, then the original rationale for such conditions no longer applies. There is a manifest public interest in maintaining the continuity of R&D and healthcare services provided by the global pharmaceutical and medical device industries, and any abrupt changes to the ability of these companies to transfer data outside of the EU will have significant operational impacts. This applies not only to the ability to transfer patient data but also to data concerning researchers, support technicians, and all the other data flows that go into the operation of a global company in the 21st Century.

C. Contractual and organisational safeguards can be important measures to ensure a level of data protection essentially equivalent to that required under EU law.

The EDPB appears to view contractual and organisational safeguards as inadequate to address the risk of foreign public authorities gaining access to data transferred from the EU (see para. 48). This view appears to be based on the assumption that contractual and organisational safeguards do not impact whether foreign public authorities are legally able to access transferred data, only technical safeguards can prevent such access. However, contractual and organisational safeguards can be important measures to prevent a foreign authority from being able to legally access the data in the first place. In this case, contractual and organisational measures are implemented not as a *consequence* of the CJEU's Schrems II judgment but rather as a *condition* to avoid triggering the need for other supplementary measures.

The question of whether contractual and organisational measures can effectively prevent a foreign public authority from legally gaining access to transferred data ultimately requires an analysis of the foreign law in question. In some cases, legal control (and, conversely, lack of legal control) may be determinative of whether a party asked to provide a public authority with data is obligated to comply and whether other third parties (e.g.,

[4] Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 (adopted 25 May 2018) at pp. 4-5.

[5] The Guidelines 2/2018 acknowledges that the Art. 49 derogations are not expressly limited in this way but argues that 'the very nature of the derogations as being exceptions from the rule' requires such an interpretation. Id. This has the effect of supplanting the lawmaker's reasoned judgment of when these derogations should apply with the EDPB's own subjective opinions.

an EU data exporter) have a legal right to intervene to prevent disclosure. In these circumstances, contractual measures can be critical to establishing legal control (and lack of legal control) of the data. For this reason, we encourage the EDPB to re-consider its assessment of the utility of contractual and organisational safeguards and to revise Use Cases 6 and 7 to account for these scenarios.

D. Pseudonymisation can provide an effective supplementary measure, but data minimisation safeguards short of pseudonymization can also be effective in some scenarios.

We agree with the EDPB's conclusion that pseudonymisation of data can be an effective supplementary measure where the additional information necessary to identify data subjects is maintained separately and securely. The EDPB appears to base this conclusion on the data not being identifiable to the foreign public authority without access to the additional information. There can be circumstances, however, where data minimization safeguards short of pseudonymisation can also be effective.

In some cases, removal of certain data elements can take a dataset outside of the scope of what foreign public authorities are authorized to access. A simple hypothetical may be helpful to illustrate this point: Imagine a foreign law that grants intelligence agencies the authority to access information containing target names. If names are removed from the target dataset before it is transferred – even if other identifiers remain – the data would no longer be susceptible to access by foreign public authorities.

In fact, the hypothetical above reflects how one of the laws at the centre of *Schrems II* actually operates in practice based on official policy statements. The targeting criteria used to limit collection of data under Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) means that only data containing specific communications identifiers (such as an email address or phone number) fall within the scope of collected data. Clinical research data is key-coded, meaning that direct identifiers such as name, address, phone number, email address, and other contact information has been replaced with a code. The clinical investigators at each site maintain the keys to re-identify clinical study participants. These keys are required to be maintained securely and in confidence. Key-coded clinical research data does not contain the types of 'targeted selectors' relied upon by US government agencies to identify communications that relate to a foreign intelligence surveillance target. Thus, key-coded clinical research data falls outside the scope of data collected under FISA Section 702. In fact, there are no known instances of Section 702 being used by the US government to access clinical research data transferred from the EU.

We suggest that the EDPB add a Use Case that addresses how laws like FISA Section 702 operate in practice and the data minimization steps that organisations could take to avoid the application of such laws (i.e., the removal or encryption of 'targeted selectors' like name and contact information).

E. Additional Comments

We recommend that the EDPB clarify these additional aspects of the document:

- 'Case-by-case' assessment of data transfers does not require a separate documented assessment of each individual data transfer where transfers of a similar nature and that present similar risks are assessed together as a category.[6] The level of analysis suggested by the EDPB as necessary will already incur significant costs, and further consideration should be given as to how these costs could be reduced. We encourage the Board to consider expanding the list of resources in Annex 3 (concerning

[6] *Cf*. GDPR Art. 35 concerning data protection impact assessments ('A single assessment may address a set of similar processing operations that present similar high risks.')

'Possible Sources of Information to Assess a Third Country') to assist organizations in conducting assessments.

Conclusion

We appreciate the EDPB's efforts to identify supplementary measures that can be used to ensure a level of data protection essentially equivalent to the level guaranteed under EU law. It is critically important to the health of EU patients that pharmaceutical and medical device companies are able to transfer personal data to jurisdictions outside of the EU, including to jurisdictions that have not received an adequacy designation. The attached paper explains the importance of these transfers, focusing in particular on transfers between the EU and the United States.