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 <u>not</u> 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.

Innovation Without Borders:
The Importance of Transatlantic Data Flows to Healthcare Innovation and Delivery

Discussion Paper

By

AdvaMed (the Advanced Medical Technology Association in the US)

EFPIA (the European Federation of Pharmaceutical Industries and Associations)

IPMPC (the International Pharmaceutical & Medical Device Privacy Consortium) and

MedTech Europe (the European trade association representing the medical technology industry)

21 December 2020

The judgment of the Court of Justice of the European Union ("CJEU") in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) (the "Schrems II" case) has created legal uncertainty around the future of international transfers of personal data from the European Union to the United States and other third countries. There is a risk that data protection authorities across Europe will interpret and enforce the judgment differently and that some authorities might order the suspension of certain transfers.

The suspension of data transfers critically needed by pharmaceutical and medical device companies would have serious consequences impacting both healthcare innovation and healthcare delivery. These activities would be made more difficult at a time when healthcare systems are already under tremendous stresses due to the COVID-19 pandemic. Thus, while *Schrems II* has created many uncertainties, one thing *is* certain — **patient care will suffer if life sciences companies lose the ability to transfer personal data from the EU to US.**

The transfer of data between the EU and the US for pharmaceutical and medical device development and support purposes serves the public interest in the protection of human health. These data transfers are crucial to continued delivery of life-saving health care services and innovation to address unmet medical needs. Numerous safeguards ensure that the data transferred is used only for permissible purposes. And importantly, there is no reason to believe these transfers pose any of the risks to privacy that were of concern in the European Court of Justice *Schrems II* judgment.

The undersigned organizations urge that policymakers and data protection authorities understand the importance of continued data transfer in health care between the United States and Europe and work to ensure that these essential activities are not disrupted while revisions are adopted or a successor is developed to the EU-U.S. Privacy Shield Framework.

Data Transfers Between the United States and Europe

The continued ability to transfer patient-related data between the United States and Europe is critical to the research and development of new medical products, monitoring the safety and effectiveness of existing marketed products, and providing support services for medical technologies currently in use. These important and necessary data flows go in both directions, and patient care will inevitably – and needlessly – suffer if restrictions on transatlantic data transfers are imposed without due consideration of the facts and circumstances of each type of data transfer.

In order to be able to effectively and efficiently develop, manufacture, and distribute drugs and medical technologies, life science companies need to be able to operate and collaborate on a global scale. Beyond the need to transfer patient data, pharmaceutical and medical device companies that operate globally need to be able to transfer a range of data concerning health care professionals, researchers, support technicians, employees, and others. The continuity of R&D and healthcare services provided by the global pharmaceutical and medical device industries depends upon these transfers. Any abrupt changes to the ability of these companies to transfer data outside of the EU will have significant operational impacts.

The European Court of Justice in its recent judgment in *Schrems II* expressed concern that certain US laws – namely the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333 – may authorize government agencies to compel the disclosure of data transferred from the EU to recipients in the US. While these laws may authorize US government agencies to obtain access to communications exchanged by or between individuals who are the target of US foreign surveillance, there are no reported cases of these laws having ever been used to obtain data transferred for pharmaceutical or medical device R&D or service delivery. In fact, there is no reason to believe that these data flows present the types of risks to privacy that were of concern to the European Court of Justice:

- **Clinical Study Data:** Clinical study data is key-coded at the study site and reported to the study sponsor (i.e., the pharmaceutical or medical device company who is undertaking the research) in this key-coded form. Key-coding involves replacing all direct identifiers with a subject identification code that is maintained confidentially at the study site. Key-coded clinical study data does not contain any of the identifiers that are used by US intelligence agencies to identify communications of foreign intelligence interest (e.g. name, address, phone number, email address, etc.). The European Data Protection Board (EDPB) has recognized pseudonymization of data as an effective means to ensure that data transferred from the EU to other jurisdictions continues to be protected in accordance with EU requirements.

- **Product Safety Data:** Reports of product adverse events are typically triaged on a country or regional basis. Only minimal information is then transferred globally for purposes of case analysis and reporting to health authorities. Directly identifiable patient information is rarely transferred.

- **Patient Monitoring, Product Customization, and Product Support Data:** Medical technology companies in Europe and the US take extensive steps to safeguard patient data from inappropriate access. These safeguards typically include the use of encryption and strong authentication requirements for user access. There is rarely a need to transfer directly identifiable patient information while providing remote device support. Patient monitoring and product customization services may require the transfer of more directly identifiable information, but patients are informed and, if applicable, must agree to these transfers.

From Research & Development to Product Safety

Today's pressing health concerns require global, concerted efforts to find safe and effective solutions. The COVID-19 global pandemic has highlighted the importance of global cooperation to address the threats posed to life, well-being, and economic prosperity by diseases and pathogens. Through data sharing and collaborative research, biopharmaceutical and medical technology companies worldwide are racing to develop treatments for the COVID-19 virus and vaccines to limit its spread. Right now, there is an acute need to transfer data around the world to speed the discovery and development of new life-saving and life-enhancing medical products. But this need did not start with the current pandemic and will continue long after it ends.

Global clinical studies

Development of innovative products to treat and prevent serious health conditions and diseases takes years. Products that must be effective worldwide require the input of scientists worldwide. To ensure that new medical products are safe and effective, data are needed from clinical studies that evaluate the use of the new product in patients. Increasingly, clinical studies involve patients and sites worldwide. Why? Global studies ensure that new products are safe and effective across different demographics, and it is more efficient to find a representative sample of trial subjects when you can conduct trials around the globe. This is especially true for studies involving rare diseases and conditions.

Demonstrating safety and efficiency

The data that is generated during global research and development (R&D) must be analysed by experts and used in submissions to health authorities and other oversight bodies worldwide. These submissions are critical to demonstrating that new therapies are safe and effective for their intended uses. Regulators and oversight bodies must receive data that allows links back to the original trial – without those links, regulators would not be able to have confidence in the scientific integrity of the research.

Monitoring and reporting

Finally, regulators and drug manufacturers still need data after a product receives clearance or is approved for marketing. Medicines agencies are charged with ensuring that the drugs and devices used to treat their citizens are safe and effective, and manufacturers of drugs and medical devices have legal and ethical duties to monitor the use of their products in real-world clinical practice and to analyse events and report safety issues to authorities. To meet these responsibilities, companies must be able to collect information on adverse events, wherever they occur, and share this information with all relevant oversight bodies wherever the product is marketed. That way, patients in every country get the benefit of a manufacturer's global experience with their product.

From Patient Monitoring to Product Maintenance & Support to Product Customization

Seamless healthcare delivery

Just as companies need to be able to transfer data across borders to conduct R&D and monitor product safety, healthcare delivery often also involves data transfers. Modern healthcare delivery relies on the availability and performance of a multitude of medical technologies. These devices are increasingly interconnected and must work seamlessly together to provide healthcare professionals with the diagnostic, therapeutic, and preventive tools they need to deliver high-quality, life-saving medical care. These medical technologies may transmit data to a centralized, global platform that can be accessed by health care providers and allows for real-time healthcare monitoring. They may also be supported by a team of global service provider personnel to ensure continuity of operations and optimal performance.

Remote patient monitoring

Remote patient monitoring technologies have been shown to be effective in managing chronic disease and post-acute care. They can provide health care professionals with information to enable early detection of health events so that proactive interventions can be prescribed. They can also be used to alert caregivers to situations requiring immediate medical attention. Many medical devices on the market today come with remote communication abilities embedded or available as optional attachments. A central database may be used to cost-effectively provide remote patient monitoring services to health care providers around the world.

Remote service

Remote service is the delivery of hardware and/or software system support, maintenance, and troubleshooting from a location beyond the healthcare delivery organization's site. Remote servicing capability has become common for most IT-based medical equipment. Remote servicing allows an equipment service provider to more efficiently monitor system performance and perform maintenance, enabling early detection and correction of potential hardware and/or software problems that could jeopardize the correct operation or continued availability of the device. It also allows remote service technicians, in the event of a system failure, to assess the severity of the problem and determine possible solutions. This can be critical when a failure occurs during a medical procedure and the healthcare provider requires immediate assistance. Finally, it enables service provider staff to more effectively provide support information and advice when on-site visits are costly or impractical. Maintenance and support of today's highly sophisticated medical devices requires specialized knowledge and training, and a global team of support professionals can most cost-effectively provide this support on a 24/7 basis.

Patient-Customized Treatments

Life science products increasingly require sharing and using patient data so that treatments can be customized to particular patients. From sizing of a prosthesis to tailored therapeutics, there is an ongoing need to exchange patient information so as to optimize healthcare delivery.

Conclusion

The life science industry in the EU and the US is committed to the highest legal and ethical standards for handling health data and reckons that the concerns of the European Court of Justice Schrems II judgment do not apply to the transfers of health data from the EU to the US. The signing organizations would like to re-iterate the importance of the seamless continuation of health data transfers between the EU and the US for the interest on patient safety and uninterrupted healthcare delivery until revisions are adopted or a successor is developed to the EU-U.S. Privacy Shield Framework.

We remain at the respective authorities' disposal for any possible questions.

For more information:

Please contact Peter Blenkinsop of the IPMPC Secretariat by email at peter.blenkinsop@faegredrinker.com.

About AdvaMed

The Advanced Medical Technology Association (AdvaMed) is a trade association representing manufacturers of medical devices, diagnostic products, and medical technology. AdvaMed's member companies produce the innovations that are transforming health care through earlier disease detection, less invasive procedures and more effective treatments. AdvaMed has more than 400 member companies, ranging from the largest to the smallest medical technology innovators and manufacturers.

For more information, visit www.advamed.org.

About EFPIA

The European Federation of Pharmaceutical Industries and Associations (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 our members to innovate, discover, develop and deliver new therapies and vaccines for people across Europe, as well as contribute to the European economy.

For more information, visit www.efpia.eu.

About IPMPC

the International Pharmaceutical & Medical Device Privacy Consortium (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.

For more information, visit www.ipmpc.org.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our members are national, European and multinational companies as well as a network of national medical technology associations who research, develop, manufacture, distribute and supply health-related technologies, services and solutions.

For more information, visit www.medtecheurope.org.