Response to European Data Protection Board (EDPB) Consultation on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

21 December 2020

MedTech Europe welcomes the opportunity to provide comments to the EDPB's Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the "Recommendations").

Hereby, we aim to provide reflections and specific recommendations for increasing the impact and usability of the Recommendations.

What the EDPB Recommendations mean for MedTech Europe members

Medical technologies ("medtech") cover products, services or solutions used to save and improve people's lives and which can be used in a care setting, such as disposables, diagnostics, capital equipment and surgical innovations, through to implant technology, biomaterials and connected health IT such as eHealth, mHealth, human genome decoding, disease prediction, biobanks, biomarkers and many more. These products and solutions, more often than not, rely on the collection, analysis, and sharing of health data, which is by nature personal data, to better understand diseases and treat them as part of an efficient and effective healthcare system.

The continued ability to transfer **patient-related data** between the United States and Europe, and not only, is critical to the **research and development of new medical products, monitoring the safety and effectiveness of existing products on the market, and providing support services for medical technologies currently in use**.

The suspension of data transfers critically needed by pharmaceutical and medical device companies would have serious consequences impacting both healthcare innovation and healthcare delivery, while creating a risk to patient safety. These activities would be made more difficult at a time when healthcare systems are already under tremendous stresses due to the COVID-19 pandemic. **For more information on the importance of the data flow between Europe and the United States, please refer to the Annex.**

In this respect, MedTech Europe **would also like to make a reminder that the right of access to preventive healthcare and the right to benefit from medical treatment are recognised rights under Article 35 of the EU Charter of Fundamental Rights**. Any interference with these rights will need to be carefully **balanced** against the risks posed by international personal data transfers.

We have therefore prepared a list of concerns and suggestions for the EDPB to consider when preparing its final recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

General comments

- The EDPB Recommendations seem to take an approach that goes beyond the legal requirements imposed by the GDPR.
- The Recommendations do not acknowledge that many countries around the world have data protection laws similar to the GDPR, such that the preservation of individuals' rights are independently overseen by courts and have remedies under such laws available to them, yet the Recommendations do not mention whether countries with laws similar to the GDPR would result in lessening the burden on organisation in relation to carrying out an assessment of national security laws of all countries to which personal data may be imported.
- Generally, the Recommendations **appear to outsource to the private sector a political function**; namely assessing the laws of foreign nations, which can be a difficult and onerous task and one that is primarily a trade and issue of international comity.
- The EDPB Recommendations **impose additional obligations on data exporters regardless of them being controllers or processors, large or small and medium-sized enterprises (SMEs)**. Though, they **should serve as support and guidance for the interpretation of the GDPR**, rather than imposing additional obligations on data exporters.
- The EDPB Recommendations also seem to be shifting away from the risk-based approach whereby compliance with the GDPR has been historically based on impact assessments (including assessment of necessity and proportionality, as well as appropriateness of organisational and technical security measures) and requiring data exporters to conduct exclusively objective assessments of third country laws for the purposes of international transfers. For example, the effect of a shift away from a risk-based approach is that the type of personal data in scope of a transfer appears to be irrelevant; if a country's laws do not meet the Essential Elements, then a transfer may not take place even where the risk to the personal data, such as would be the case in relation to medical devices, is exceedingly low. For example, national security laws seek to understand communications between individuals involved in espionage, terrorism or other matters of national security; not personal data processed for the purposes of medical diagnosis, treatment or management of a medical condition, which generally would not contain data of relevance to identify terrorists and the likes or relate to issues of national security. **MedTech Europe would recommend that the EDPB updated the Recommendations in the light of the risk-based approach, as foreseen by the GDPR.**
- The EDPB should also seek to align its approach with that of the lawmakers (see Article 35 of the GDPR) and not require data exporters to conduct assessments on a case-by-case basis. In addition, MedTech Europe would recommend that the EDPB acts in the spirit of the GDPR and allows organisations to conduct a single assessment for similar processing operations that present similar high risks.

Step 1: Know your transfers

Full awareness of your transfers (paras. 8-13)	While it is welcomed to know that controllers and processors can build on their Records of Processing Activities (hereafter "ROPAs") for fully understanding one's transfers, it will help if **the EDPB clarifies why such exercise is required**. **Article 30 of the GDPR** specifically states the required contents of the ROPA held by controllers and processors, respectively. **It is unclear what the EDPB's expectations are in this respect and how data exporters are expected to "build on" their ROPA**. **We would recommend clarifying this aspect or delete this part of the Recommendations.** In particular, onward transfers in an **intra-group arrangement** is an ever-evolving situation. Given organisations are already required under the GDPR to keep their ROPA up to date, and companies have invested resources to comply with this. The ROPA is a live document and offers transparency and visibility over an organisation's transfers. **The EDPB should not require companies to go beyond the GDPR requirements.** Otherwise, clarification and practical examples, in particular around how companies should consider onward transfer situations in an intra-group context in order to meet the EDPB expectations, would be welcomed. Additionally, Article 30(5) of the GDPR assists enterprises and organisations employing fewer than 250 persons (under certain conditions), by exempting them from the requirement to keep a ROPA. It is not clear whether such enterprises and organisations are now expected to create and keep a ROPA to gain full awareness of their transfers. Such requirement would impose a high burden on such small to medium sized enterprises and the EDPB should consider a similar approach to the approach already laid down in the GDPR. The EDPB mentions in footnote 22 that "remote access by an entity from a third country to data located in the EEA is also considered a transfer". This seems to be somewhat contradicting the European Union's Court of Justice decision in case C-101/01 (albeit based on the old Directive 95/46), where the court decided that data uploaded on an online platform and then accessible to entities or individuals in third countries should not be considered a transfer for the purposes of data protection laws. If such a view would be taken, this would give the GDPR a regime of general application regarding data placed on the internet and would mean that each time data is uploaded on online platforms and is accessible via technical means from third countries, a transfer would take place. In practice, it is unreasonable to interpret this as the intention of the lawmakers. The EDPB is urged to clarify the reference in footnote 22 regarding remote access.
No transition period (para. 12)	MedTech Europe would recommend the **EDPB to reconsider implementing a transition period.** The practical implications of not having a transition period is such that suspending transfers will be **very burdensome on organisations and could effectively interfere with organisations' right to be free to conduct a business**, recognized as under Article 16 of the EU Charter of Fundamental Rights. Any

	interference with this right will need to be **carefully balanced against the risks** posed by international personal data transfers. **The EDPB should acknowledge that businesses need time to ensure appropriate compliance and proper implementation with its recommendations.** The **assessment of a third country's laws is neither an easy nor short process**, especially for the private sector (see more below). Such suspension of transfers will be highly detrimental to the progression of medical research, continuity of care (e.g. if specialised US teams would be not able to provide remote support) or vigilance reporting and would be contrary to public interest and the wider benefit of humankind. Similarly, international organisations may use non-EU based centralised back-up systems and forcing organisations to switch to EU-based providers will only impose a high burden, both in terms of time and costs, which will be detrimental to the main objective of medicine. 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, and such a situation is recognised within the GDPR**. Requesting the suspension of such transfers of data will be detrimental to humankind and will halt the progress that has been made thus far in advancing a vaccine and/or the ability to test for antibodies and antigens for the COVID-19 virus. **MedTech Europe urges the EDPB to consider allowing for a transition period prior to the implementation of the EDPB Recommendations, to allow organisations time to consider the laws of the third country where they are currently transferring data to, and have time to negotiate supplementary measures with their data importers.**

Step 2: Identify the Transfer Tools

Adequacy Decisions (para. 19)	**MedTech Europe welcomes the acknowledgement from the EPDB that where a country has been deemed adequate that no further assessment is required.**
Derogations (paras. 24-26)	With regards to the part on the Derogations, **the EDPB guidance appears to go beyond the text of the GDPR by stating that Art. 49 derogations have an exceptional nature**. Both the text of the GDPR and Recital 113 make it clear that **non-repetitive and limited transfers based on legitimate interests are meant to**

	be exceptional, **not the article as a whole,** despite previous guidance to the contrary. For example, Recital 111 uses the words "occasional" and "exceptional" for transfers necessary for contractual or legal claims, rather than non-repetitive transfers. This clearly shows the lawmakers intention to differentiate between the derogations and in what situations they should be relied on. The **MedTech industry relies heavily on consent to both process and transfer personal data and the right of an individual to exercise their freedom of autonomy should not be undermined by qualifying use of the derogations as exceptional. MedTech Europe welcomes the EDPB guidance which acknowledges that where a derogation is used for the transfer of personal data, then like an adequacy decision, there is no obligation to carry out an assessment.**

Step 3: Assess whether the Article 46 of the GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

Standard of assessment (paras. 28-44)	The EDPB Recommendation suggests that the data exporters will need to determine: • Whether the applicable laws specific to the data transfer are likely to require the disclosure of transferred data to, or permit access of data by, public authorities (e.g. for purposes of national security, law enforcement or regulatory supervision); and • Whether these requirements or powers are limited to what is "necessary and proportionate in a democratic society". This will need to be measured against the EDPB European Essential Guarantees, which set out expectation of surveillance laws to meet the EU standards. **Step 3 of the EDPB Recommendations sets a very high bar for exporters, regardless of their size, as data exporters will not only need to review the data protection laws of the third country, but also national security, surveillance laws and local practices of enforcement authorities.** In particular, **small and medium-sized companies (SMEs)**, such as independent laboratories, will likely not have the necessary resources, both in terms or people and capital, to conduct such assessments. Further guidance will be welcomed as to what data exporters are required to do if they do not have the necessary resources to conduct such assessments, especially as such assessments are required for each transfer on a case-by-case basis. In addition, **Step 3 does not mention that many countries around the world have data protection laws with protections equivalent to the GDPR, such as countries that have ratified Convention 108**. Where a country has such laws, then organisations should not be required to carry out an assessment of that country's data

	protection laws, particularly where the data protection law provides for independent oversight and affords data subject access to remedies.
Going beyond *Schrems II* and the GDPR (paras. 28-44)	The EDPB Recommendations were issued as a response to the invalidation of the U.S. Privacy Shield in the *Schrems II* case. The *Schrems II* case invalidated the U.S. Privacy Shield due to the US surveillance laws. However, the **EDPB Recommendations now suggest that data exporters are required to assess all applicable laws and relevant rules of a general nature** (insofar as they have an impact on the effective application of the safeguards contained in Article 46 of the GDPR transfer tool and the fundamental rights of the individuals) of the importing country. MedTech companies, and other regulated organisations, must always **collaborate with their regulators** and other oversight bodies, in order to ensure compliance with their **regulatory obligations**. In the medtech industry, this is even more important given the impact such products have on individuals and healthcare around the world. **Not being able to share information with local regulators will be highly detrimental to the benefits such transfers bring, as new products would not be able to be certified or would not be able to be used worldwide.** Additionally, at paragraph 38 of the EDPB Recommendations, the EDPB guides data exporters to the elements listed in Article 45(2) of the GDPR to assist them in determining the adequacy of the importing country's laws and the protection offered to individuals. Article 45(2) of the GDPR covers the elements that the European Commission must consider when they are assessing the level of protection in preparation for an adequacy decision. While the additional guidance is beneficial, **it is not reasonable and proportionate for the EDPB to expect data exporters to have the level of expertise the European Commission has when making their own assessments of adequacy.** Data exporters do not benefit from the same tools and resources that are available to the European Commission. Further, the European Commission can take several years to review a country's laws and practices to make a decision as to whether that respective country will be considered "adequate". We have now seen in practice (both in *Schrems I* and *Schrems II*), that even with all the resources available to European Commission, an adequacy decision can still be overturned by the CJEU. **MedTech Europe would welcome if the EDPB re-considered the reference to laws and rules of a general nature and provided a narrower description of the relevant laws and rules for the assessment of third country laws**, for example which would focus on surveillance laws and aligns more closely with the CJEU ruling in *Schrems II*. In the absence of this, **the EDPB Recommendations seem to suggest that data exporters would be expected to assess the entire legal system of a third country as to whether it is adequate or not, task which, under the GDPR, has been left to the European Commission**. In any case, an organisation should not be made to

	conduct any analysis of the same level that the EC undertakes when deciding on adequacy. Clarification from the EDPB in this respect will be most welcomed.
Risk based approach (paras. 42-43)	The EDPB Recommendations then go further and suggest that data exporters, in situations where legislation in the third country may be lacking, or is not sufficiently clear, should look at "other relevant and objective factors", e.g.: • Elements demonstrating whether a third country authority will seek to access the data, in light of reported precedents, legislation and practice; and • Elements demonstrating a third country authority will be able to access data through the data importer or through direct interception of the communication channel, in light of reported precedents, legal powers, and technical, financial and human resources at its disposal. While the EDPB mentions that data exporters should not rely on subjective factors such as the likelihood of the public authorities' access to the data, such type of other relevant information based on precedents, practice, or technical, financial and human resources are subjective factors in itself. **A sensible approach would be to use those to factors to be able to prove the opposite scenario as well: that third country authorities will not, or will very likely not, seek access to the data an exporter is transferring.** In such situations, it will be reasonable for organisations to conclude that such a third country will provide essentially equivalent levels of protection to those found in the EU. **Indeed, MedTech Europe considers that this will allow for a full, practical analysis, which will benefit the medtech industry and patients worldwide, rather than a simply theoretical one.** For example, 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 authorise government agencies to compel the disclosure of data transferred from the EU to recipients in the US. While these laws may authorise 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 (this is also supported by the white paper prepared by the US government as a response to the *Schrems II* decision). 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 CJEU: • 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.).

	• 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 and Product Support Data: Medical technology companies 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. Patient monitoring services may require the transfer of more directly identifiable information, including for patient safety issues and compliance with the medical devices regulatory framework. • Employee Data: In the context of international commerce, companies are becoming more and more global. As such, group companies located outside the EEA may need access to employees' data due to legal or health and safety reasons, or simply due to usual business needs. **Not following a risk-based approach will undoubtedly affect the normal business dealings of organisations, and in particular global research around the world.** The ability to **collaborate in the medical field** is perhaps now more important than ever, and the EDPB should re-consider allowing data exporters to engage and rely on a risk-based assessment. An in-depth assessment of the importing country's laws based on reviewing the applicable laws and rules of general nature will involve a great amount of resources, which will need to be engaged in a very short timeframe. **Additionally, the scope of third countries laws regarding public authorities' access to data is not always clear, so there is a risk of divergent assessments between organisations.** The EDPB is urged to consider the **practical impact such a requirement has on organisations and how this will affect the medical research and collaboration, as well as the marketing on non-EU products that have a CE mark**, which is paramount at this time. It is important that research and development teams are placed around the world in order to ensure the best data is analysed, based on a variety of resources. **The EDPB should consider and provide reasonable recommendations on how many resources the data exporters are expected to invest in these assessments.**

Step 4: Adopt supplementary measures

Supplementary measures (paras. 46-49)	While the EDPB recognises the variety of supplementary measures available to data exporters (i.e. technical, contractual and organisational), the **EDPB also seems to suggest that contractual and organisational measures will not be sufficient** unless coupled with appropriate technical measures. Such a decision will depend on the laws of the importing country, and the public authorities' rights under such laws.

	It is not clear why contractual and organisational measures alone are so easily dismissed, when they may be key in certain situations. For example, Art. 47 and 48 of the GDPR recognise such measures are suitable for international transfers, without the need for any other supplementary measures. Therefore, the type of supplementary measures to be implemented should be determined by the data exporter following their assessment of the importing country's laws using a risk-based analysis. **It appears that the EDPB's recommendations allow for and steer towards fragmentation, rather than harmonisation, regarding the implementation of the GDPR and the safeguarding of data. MedTech Europe recommends clarifying those aspects.**
Technical measures (paras. 45-54, 72-91)	The EDPB Recommendations and case studies, albeit non-exhaustive, are very detailed. Given the high burden imposed on data exporters, the **EDPB should consider providing more varied examples on which data exporters can turn to**. The EDPB should consider less specific and rigid examples; otherwise, there is a risk the solutions suggested by the EDPB may be interpreted as the only acceptable solutions. For example, **data anonymization or data minimization are other means by which the data subject's rights can be protected which was not mentioned in the EDPB Recommendations.** Removal of certain data, such as names, can take the data outside the scope of the surveillance agencies interest. Surveillance agencies would not be interested in a data set which does not contain any names, and only contains medical data in relation to reactions to a new medicine. In particular, **the inclusion of negative examples, such as case studies 6 and 7** (see below) **does not assist organisations with ensuring compliance, nor understanding how they could legitimise such transfers.** The EDPB Recommendations make reference (at para. 78) to the requirements of Article 32 of the GDPR. **Article 32 of the GDPR** requires data controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, by "taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". However, **the EDPB Recommendations do not allow for a risk-based approach**. **It is unclear whether the EDPB now expects data exporters to implement such measures regardless of the costs of implementation and the risk of infringement of data subjects' rights and freedoms. Further clarification would be welcomed.** The GDPR therefore requires data controllers and processors to assess any required supplementary measures based on the **risk of the transfer**. The EDPB is **urged to take this into account when it revises the EDPB Recommendations following the end of the consultation period**. Not allowing organisations to take into account the costs of implementation and engage in a risk-based approach when it comes to

	considering and implementing the necessary measures will have an adverse impact on data exporters' businesses.
Annex 2 (paras. 69-137)	It would be very helpful if the **following statements could be supplemented by the text** "*as it ensures that data transferred to the recipient country does not constitute personal data.*": • then the EDPB considers that the encryption performed provides an effective supplementary measure (Use Case 1); • then the EDPB considers that transport encryption, if needed in combination with end-to-end content encryption, provides an effective supplementary measure (Use Case 3); • then the EDPB considers that the transport encryption performed provides an effective supplementary measure (Use Case 4); • then the EDPB considers that the split processing performed provides an effective supplementary measure (Use Case 5).
Flawlessness (paras. 79, 84)	The EDPB Recommendations provide in their case studies the requirement that "any encryption mechanism is flawlessly implemented". **In practice, flawless implementation is unlikely to be achieved due to constant technological advancement**. Additionally, requiring data exporters and importers to ensure the implementation of supplementary measures in a **short period of time, with no transition period, will not provide enough time for data exporters and importers to research into the best implementation methods for their particular transfers.**
Keys to encryption and any additional data to be kept by the data importer, within the EU or within a country subject to an adequacy decision (paras. 79, 84, 85)	The EDPB's recommendation that keys to encryption and any additional data to be kept by the data importer, within the EU or within a country subject to an adequacy decision will impose a high burden on data exporters, as they will need to engage into contract negotiations with various third parties and incur costs for their services. Nevertheless, **the GDPR does not require encryption keys to be kept in the EU.** Additionally, the CJEU has mentioned in the *Schrems II* decision: *Invariably, research data are uniquely key-coded at their origin by the principal investigator so as not to reveal the identity of individual data subjects. Pharmaceutical companies sponsoring such research do not receive the key. The unique key code is held only by the researcher, so that he or she can identify the research subject under special circumstances (e.g., if follow-up medical attention is required). A transfer from the EU to the United States of data coded in this way would not constitute a transfer of personal data that would be subject to the Privacy Shield Principles.* **The EDPB is urged to take this into consideration and the effect the Use Cases described below would have on MedTech organisations.**
Use case 6 (paras. 88-89)	Use case 6 of the EDPB Recommendations essentially impose a full ban on the use of cloud service providers or other processors which require access to data in the clear. A large number of organisations use cloud service providers or other processors to store personal data. Essentially, data exporters will have no other choice than moving to service providers who operate solely within the EEA, without any form of e.g. outside

	EU remote support for technical or maintenance reasons or trouble shooting, or within countries that are subject to an adequacy decision. **In practice, these restrictions seem to qualify (at least de facto) as a data localization requirement.** This is not something imposed by the GDPR, and it is another instance where the EDPB **Recommendations seem to go above and beyond what the GDPR requires** and is **beyond what would be required by the CJEU ruling**. Moreover, such a change is not as easy to make as it would involve choosing a new service provider and negotiating a contract with them, and terminating the contract with the current service provider. Such termination may incur **additional costs for the data exporters,** in particular if the termination is done at short notice. We request that the **EDPB re-considers their position on the above use case and provide practical recommendations as to what data exporters that find themselves in such situations should do to ensure compliance.**
Use case 7 (paras. 90-91)	This is common in an intra group scenario, where a parent company will likely be required to have remote access to its employees' data in the clear. **MedTech Europe 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 medical technologies may need to transmit data to a centralized, global platform that can be accessed by health care providers and allows for real-time healthcare monitoring. This is necessary to ensure that **continuity of operations** and optimal performance around the world. Additionally, remote patient monitoring technologies have been shown to be effective in managing chronic diseases and post-acute care, and can be very efficient in alerting caregivers if a patient requires immediate medical attention. A central database is in the interests of patients and health care providers, as this can provide a cost-efficient and always available method of remote patient monitoring, including responses 24 hours / 7 days a week. **The EDPB is urged to re-consider this scenario and provide a practical solution for companies that find themselves in such contractual and organisational arrangements**.
Transparency obligations (paras. 100-101)	The EDPB Recommendations suggest that data exporters may include an obligation on data importers to provide them with information on access to data by public authorities, based on the data importer's **"best efforts".** There are two issues arising from this requirement. In a contractual negotiation, agreeing to "best efforts" is unlikely. Best efforts impose a high standard on parties and such clauses are not common in contracts. Parties usually agree to **"reasonable efforts".** Even if the data importer was to provide such information to the data exporter, the data exporter would still be required to make **additional enquiries and incur a vast amount of costs.**

	The EDPB should consider balancing such contractual obligations and expectations from a practical perspective. The EDPB should also clarify whether data exporters can fully rely on the information received from data importers, and in what circumstances data exporters are required to follow up with additional independent research into the importing country's laws.
Transparency obligations (paras. 110-111)	While the suggestion of implementing a Warrant Canary method is useful, the EDPB should consider the practical effects of implementing it. The data importer will likely seek to charge a fee for this service, which will in turn result in additional financial burden on the data exporter. The data exporter will then also need to implement a system to automatically monitor these notifications.
Adoption of standards and best practices (para. 135)	The EDPB Recommendations acknowledge that adherence to data security and privacy policies, based on international standards or EU certification or codes of conduct, "in accordance with the risk of the categories of data processed and the likelihood of attempts from public authorities to access it" are suitable supplementary measures. Such a risk-based approach is considered adequate and in line with the GDPR requirements. **The EDPB should consider adopting such approach throughout their final recommendations**. This will ensure companies can continue their business activities, while adequately safeguarding data subjects' personal data and personal freedoms.

Step 5: Procedural steps if you have identified effective supplementary measures

Consultation with supervisory authorities (para. 57)	Supplementary measures are meant to be complementary to the SCCs (or any other transfer mechanism) and enhance the protection of individuals. We would welcome **practical examples** of when the EDPB considers that supplementary measures could **"contradict" both directly and indirectly the SCCs**.

Conclusions

Concluding, we would appreciate if the above considerations are taken into account by EDPB, whether it is to update these Recommendations or for the development of additional ones, perhaps more focused on clinical/ healthcare research, and we **would welcome a further discussion on the specificities of the medtech industry**.

About MedTech Europe

MedTech Europe is the European trade association for the medical technology industry including diagnostics, medical devices and digital health. Our purpose is to make innovative medical technology available to more people, while helping healthcare systems move towards a more sustainable path. 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, please visit www.medtecheurope.org.

If you have any further questions, please reach out to:
Caterina Marcon
Officer Legal & Compliance, MedTech Europe
c.marcon@medtecheurope.org

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.

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.