Joint medical technology industry perspective on the Data Act

9 November 2023

MedTech Europe and COCIR are partnering to present a joint medical technology industry perspective on the final agreement of the Data Act. Both organisations highlight the need for a future-proof framework that preserves incentives for industry to invest in methods of generating value through data, in a balanced and proportionate way, for the benefit of patients and healthcare systems.

Applying the Data Act requirements to the health sector brings unique and highly complex challenges with it. Connected medical technologies are widely used in healthcare and enable diagnosis, better care and decision-making, which can translate into improved patient outcomes. Data generated by the use of medical technologies is part of the authorised use under the Medical Devices Regulation (MDR)[1] and the *In Vitro* Diagnostic Medical Devices Regulation (IVDR)[2] which set out comprehensive requirements for product design, but also patient safety and security protections.

The scope of the Data Act is very broad, which requires further guidance in terms of which data needs to be made available under which circumstances, and how to protect data that is highly sensitive. The scope of data to be provided is unlimited in cases of emergencies, with no restrictions on further sharing with third parties for purposes other than public emergency management, which requires further clarification. Furthermore, it will be essential to contextualise the Data Act in view of forthcoming sector-specific legislation (such as the European Health Data Space Regulation (EHDS)) to have a better understanding about the interplay of provisions and alignment in terms of definitions.

.

Data sharing obligations with regard to sectorial legislation

Trust in digital health and health data sharing is paramount. As a result, medical technologies are comprehensively regulated by the MDR and the IVDR, which require that only safe, secure, and well-performing devices are placed on the EU market. Additionally, the GDPR[3] is in place to ensure the protection and secure processing of personal data, and we anticipate that specific healthcare-related legislation, such as the European Health Data Space (EHDS), will be established in the foreseeable future.

- **The obligation to share data under the Data Act should in no way contradict or compromise the obligations for medical technologies required under other EU legislation, which may have implications on patient or device safety.**

In principle, we support the inclusion of the possibility for data holders and users to agree contractually on restricting or prohibiting access to data for security reasons, particularly if such processing might result in serious adverse effects, especially on “the health, safety or security of human beings”. With healthcare

[1] Medical Devices Regulation: Regulation (EU) 2017/745

[2] *In Vitro* Diagnostic Medical Devices Regulation: Regulation (EU) 2017/746

[3] General Data Protection Regulation (EU) 2016/679

delivery remaining particularly vulnerable to harmful interference, it will be crucial to mitigate the increased risk of cyberattacks and other related threats. A possibility to restrict data sharing outside the confines of the secure and regulated sectoral framework is needed, along with safeguards for protecting patients and hospitals from adverse impacts on the safety and security of highly sensitive data.

- **We advocate for an interpretation that includes the safety, performance, and efficacy requirements of medical technologies, given their direct impact on the health and safety of patients.**

The Data Act still leaves several (cyber) security, privacy, and safety concerns unaddressed. Without insight into the functioning of the proprietary algorithms of medical technologies, users (patients), may not be able to interpret the raw data accurately, creating a risk of incorrect diagnosis or treatment decisions. The safety of patients can also be compromised in view of the new design requirements: devices developed under the principle of "accessibility-by-design" may be less resilient and more vulnerable to security threats. Furthermore, the sharing of such data may lead to an expansion of a medical technology's risk profile and increased vulnerabilities in devices. Finally, making additional data points available can impact the functioning of the technology when this was not part of the original design and represents significant modifications for medical technologies, which could require re-certification. This would be disproportionate, due to the known challenges faced by MDR/IVDR-designated Notified Bodies.

- **More clarity on the Data Act's interplay with GDPR, MDR and IVDR cybersecurity, safety, and efficacy requirements, as well as privacy requirements, is crucial to mitigate unintended risks.**
- **Additionally, a better understanding of the interplay with upcoming sectoral data legislation, namely the EHDS, is needed.**

Protection granted by intellectual property rights and trade secrets

The objective of the Data Act is to enable innovation and with that, the protection of intellectual property rights and trade secrets protection in alignment with the existing legal framework should remain its fundamental pillar. Intellectual Property Rights and Trade Secrets underpin investments in research and innovation and play a significant role in ensuring that medical technology companies remain incentivised to improve healthcare for the benefit of European citizens and health systems.

We welcome the reference to Union and national legal acts providing for the protection of intellectual property[4]. However, our concerns persist that the Data Act could still have unintended and potentially detrimental consequences on a company's ability to protect critical intellectual property assets and trade secrets. This could consequently lead to a situation where the legal protection of intellectual property rights and trade secrets becomes subject to gradual erosion.

- In this context a rather **narrow interpretation of which data is readily available as well as the alignment with the existing legislative framework on the protection of IP and trade secrets as well as international agreements is important.**

[4] including 2001/29/EC, 2004/48/EC, and (EU) 2019/790 of the European Parliament and of the Council

We support the introduction of the right for data holders to refuse a request for data (e.g., so-called 'raw' data or pre-processed data) by users or third parties, as this data may be covered by IP rights or trade secrets. However, the high burden of proof for the data holder to "demonstrate that it is highly likely to suffer serious damage" needs to be clarified and limited to a reasonable threshold. Despite the safeguards included the scope of data sharing obligations under the Data Act is still very broad, which could put sensitive business information at risk, given the nature of data and trade secrets.

International data flows

We believe that it is important to protect the secure cross-border transfer of healthcare data, both personal and non-personal, that allows the aggregation of data from different countries, enabling research and scientific advances for medical breakthroughs. We are concerned about the risk of imposing localisation and sovereignty provisions and seek alignment with the existing frameworks that already provide solid safeguards for the international transfer of data.

- **Any risk of imposing data localisation and possible counter-reactions of third countries must be avoided.**

Interoperability

Provisions to ensure interoperability and safeguards for international data transfers are essential for the health technology sector.

- To realistically strive for interoperability of data, data sharing mechanisms and services, **it is important to rely on already successfully implemented fit-for-purpose and consensus balloted healthcare interoperability standards** (e.g., HL7, SNOMED, etc.). Additionally, applicable international standards need to be clearly preferred over local European standards.

Manufacturers of medical technologies heavily rely on access to diverse datasets for research and development purposes, which is supported by interoperability standards.

- **We recommend that the Data Act encourages the creation of data repositories, consortia, or other mechanisms that allow companies to access and utilize anonymised, aggregated healthcare data for research and development, like HealthData@EU.** Such initiatives should prioritise maintaining the privacy and security of individuals while providing an environment conducive to innovation and breakthrough discoveries.

Conclusion

MedTech Europe and COCIR are drawing attention to the Data Act's impact on the medical technology sector and the importance of guidance that includes the necessary clarifications and references to the safety, health, and performance of connected products as well as future sector-specific legislation, such as the EHDS.