MTE position on the Proposal on harmonised rules on fair access and use of Data (Data Act)

4 November 2022

Executive Summary

In the context of the proposed Data Act[1], which aims at ensuring fairer value allocation from data and fostering increased access to and use of data, MedTech Europe would like to highlight the need to preserve incentives for industry to invest in methods of generating value through data, in a balanced and proportionate way. Connected medical technologies are widely used in healthcare and integrated across a variety of platforms to enable diagnosis, better clinical care practice and decision making. As such, medical technologies are impacted by the provisions of the Data Act as it will require them to make data generated by the use of a product or service easily, securely and directly accessible to the user, by default. MedTech Europe, however, wants to outline that the Data Act needs to be clearer, in terms of its scope and definitions, and clearly align with existing (and future) sectoral and horizontal legislation and protect trade secrets and other intellectual property rights. The following position paper outlines MedTech Europe's position in detail and highlights the importance to consider sectoral peculiarities.

In particular, the Data Act should:

- **Recognise the complexity of the healthcare sector.** Applying the Data Act requirements to the health sector brings unique and highly complex challenges with it. Especially the fact that data generated by the use of connected medical technologies are part of the authorised use under MDR[2] and IVDR[3] which set out strict requirements for product design, but also patient safety and security protections.
- **Provide precise definitions and a clear scope.** This should be in clear alignment with existing legislation, to determine the nature of the proposal. Central definitions (e.g., 'data', 'user', 'product', 'data holder', etc.) must be clarified to avoid unintended or inadvertent consequences.
- **Take into account existing legislation.** The data-sharing obligations outlined in Chapter II of the proposed Act could compromise the safety, security and performance of medical technologies and patient data, which is required under existing EU legislation, namely the MDR, IVDR and GDPR[4]. The Data Act should therefore not oblige the manufacturers of connected medical technologies to make data available outside the confines of the secure and regulated framework. Furthermore, it should consider the technical feasibility and potential need for the recertification of medical technologies. In addition, proposed timelines for implementation may conflict with mandatory market authorisation processes under existing sectoral regulations, which could lead to negative

[1] Proposal for a regulation on harmonized rules on fair access to and use of data (Data Act)
[2] Medical Devices Regulation: Regulation (EU) 2017/745
[3] In Vitro Diagnostic Medical Devices Regulation: Regulation (EU) 2017/746
[4] General Data Protection Regulation: Regulation (EU) 2016/679

effects on the continuity of healthcare. Therefore, the Data Act should not oblige manufacturers of connected devices to make that data available, where such concerns exist.

- **Avoid the erosion of the protection granted by IP rights and trade secrets.** The Data Act must clearly define the terms for data sharing and accessibility obligations with third parties, consistent with the Trade Secrets Directive, to better protect the confidentiality of trade secrets and intellectual property. We recommend clearly exempting trade secrets from the scope of the final regulation, as is the case under the GDPR.

Furthermore, we suggest to:

- **Ensure consistency with existing rules on data protection** and introduce better alignment with concepts that also fall under GDPR, such as the concept of the data controller.
- **Seek alignment with future legislation**, such as the proposed European Health Data Space[5], including prioritisation and scoping.
- **Refine the definition of 'public emergency'** to defined cases where the sectors affected are described, clear instructions and proper guidance is given on what type of data should be disclosed and for which purposes without providing grounds for misinterpretations.
- **Prioritise the use of harmonised standards** rather than key common specifications as a default, to accurately reflect the state of the art, particularly for cybersecurity and interoperability.
- **Carefully consider the strict obligations regarding data portability for data processing services.** Especially the obligation to have a maximum termination period of 30 days to transfer all data to a competing service provider is technically unfeasible and would considerably undermine the competitiveness of EU actors' cloud offerings.
- **Avoid fragmentation** regarding the enforcement of Data Act provisions and ensure cooperation between competent authorities in the Member States.

[5] Proposal for a Regulation on the European Health Data Space

Table of Contents

Introduction

The Data Act aims to at ensuring fairer value allocation from data and fostering increased access to and use of data. Further, it complements existing legislation and other proposals intended to establish a single EU market for data. MedTech Europe shares the Commission's overarching objective to address barriers to the safe and secure sharing of data in the EU and leveraging the economic and societal potential of data.

Connected medical technologies are widely used in healthcare and integrated across a variety of platforms to enable diagnosis, better clinical care practice and decision-making, utilising the benefits of digitalisation to provide better, faster and more efficient healthcare. Medical technologies generate and use data to predict, prevent, diagnose, and treat patients. As such, medical technologies are impacted by the provisions of the Data Act as it will require them to make data generated by the use of a product or service easily, securely and directly accessible to the user, by default.

MedTech Europe believes the Data Act should preserve incentives to invest in ways of generating value through data in a balanced and proportionate way and should ensure alignment with the existing legislative framework. Particularly in health, provisions to make data directly accessible to the user and third parties may have adverse impacts on the safety, security and privacy protections afforded under the existing regulatory framework. Therefore, we call on legislators to support customised rather than horizontal measures, with full consideration given to the context in which connected devices and related services are used, the generated data, and the existing sectoral and horizontal regulatory environment when further developing a data-driven economy. In particular, sectoral legislation such as the Medical Devices Regulation ('MDR')[6], and the *In Vitro* Diagnostic Medical Devices Regulation ('IVDR')[7] should be considered. Furthermore, we want to highlight the need to align the Data Act with other existing and future legislation.

The following position paper outlines MedTech Europe's position in detail and highlights the importance to consider sectoral peculiarities.

1. The Data Act in the context of healthcare

The proposed Data Act is horizontal in nature, aiming to broadly regulate access to data from devices across EU industries and sectors, including healthcare. However, applying the requirements of the Data Act to the health sector brings unique and highly complex challenges with it. For example, the data generated by the use of connected medical devices and *in vitro* diagnostic medical devices are part of the authorised use under two sectoral EU regulations: the MDR and the IVDR. Both regulations set out strict requirements for medical technology manufacturers in terms of patient safety, security, protection against unauthorised access and availability of service and are applicable to connected medical technologies, e.g., for treatment or diagnosis. This also implies that medical technologies and the data they generate are primarily, and often exclusively, used and interpreted by healthcare professionals (HCPs) to support decisions taken throughout a patient's care pathway. Hence, they play a vital role in interpreting the data and translating them for patients. The software used for reading, interpretation and

[6] Medical Devices Regulation Regulation (EU) 2017/745
[7] In Vitro Diagnostic Medical Devices Regulation Regulation (EU) 2017/746

validation of medical data is very often also part of the regulatory scrutiny under MDR and IVDR which set out strict requirements for clinical data collection and evidence generation.

The proposed Data Act introduces obligations to make data generated by the use of a product easily, securely and, where relevant and appropriate, directly accessible to the user, by default. Given this context, MedTech Europe is concerned that not all data generated by medical technologies is fit to share in the context of the proposed Data Act. The below example aims to illustrate this:

Example: Raw data from medical technologies is not directly fit-to-share with users and third parties
Raw device data, e.g., from implanted devices such as pacemakers, produce data according to signals they receive from the patient. The raw data generated from the use of a medical technology needs to be further processed and translated (e.g., into an electrocardiogram (ECG)) by proprietary software and algorithms to ensure data quality so that the device data is 'fit for purpose'. Even after the translation, further interpretation by trained HCPs is required to derive accurate information about a particular patient.

2. Unclear scope and definitions

MedTech Europe believes, it is imperative for the Data Act to provide precise definitions and a clear scope, consistent with existing legislation. This should help determine the nature of the proposal, as well as its effective implementation. In our view, several definitions in the proposed Act require further clarification as follows:

Data

The definition of 'data' in the proposal, in Article 2(1), is overly broad for the intended nature of the proposed Act. It includes both personal and non-personal data and does not further distinguish between different types of data, creating uncertainty about the scope of the proposed legislation. Given the subject matter of the legislative proposal, it is crucial that the definition of 'data' is clear, future proof, and legally tenable.

Recital 17 creates an exception for information derived or inferred from this data, which we welcome as an important protection for innovation that is part of the connected product as offered by the data holder. However, overall, the Act fails to be clear in its scope and it is unclear if concepts of device-generated and user-generated data can be clearly separated from derived or inferred data, while applying the obligations of the Data Act.

Recital 14 includes "user actions and events", however, MedTech Europe believes that to ensure legal certainty, the definition of 'data' should be further clarified and narrowed down to data created through user actions, i.e., data actively created by the user. The finalised Data Act should not include data generated without any action by the user as such data may be subject to legal requirements relating to trade secrets and intellectual property rights. This goes for machine-generated data or for data from products interacting with other devices (e.g., IoT). In addition, while personal data is included in the definition of data, the Data Act does not provide for a legal basis to share personal data, as imposed by the GDPR.

Finally, as further explained in the section on IP, the final Data Act regulation should only apply to finished connected products, with an associated clear definition, and only to certain data that would not risk exposing proprietary information, commercially confidential data, trade secrets, and related Intellectual Property Rights (IPRs). MedTech Europe recommends that data which is not already generally available or publicly accessible, such as encrypted data, data processed locally on a device, technical data, or other data categories that may expose proprietary data, sensitive (e.g., personal) data, or trade secrets should be excluded from the scope. In addition, the final regulation should clearly identify data holders based on the notions of actual/real control and ability to make data available, where possible and within reason.

User

Article 2(5) requires clarification, given the complex nature of the healthcare value chains. Currently, it is not clear, whether a "user" is the HCP, the patient, the hospital, or another actor. Data generated by medical technologies are primarily used and interpreted by licensed HCPs, even in instances where a connected medical device may be 'worn' by a patient. Where data is used or read by patients, it will be health data already interpreted by the algorithms of the device manufacturer. In the regulated medical context, considering the patient as the 'user' of the connected device (e.g., as regards implanted devices) and hence the recipient of the 'raw' data may come with consequences not anticipated by the Data Act.

Data Holder

The final regulation should clearly identify data holders based on the notions of actual control and ability to make data available. It is unclear who would classify as a 'data holder' as the value chains in healthcare settings are very complex, e.g., hospitals can be data controllers, while manufacturers would be data processors acting upon the instructions of hospitals when it comes to the processing of personal data. MedTech Europe also suggests having a clearer definition of this concept, in line with the GDPR.

Product

The definition of '*product'* in Article 2(2) requires clarification as based on this definition any product may collect data, and it is unclear how to distinguish a '*product'* from a component and a '*related service'* in order to have clarity about the scope of the provisions. Furthermore, we suggest defining '*publicly available electronic communications service*' on its own to enable a more precise definition.

Public emergency

The proposed definition of '*public emergency'* in Article 2(10), is overly broad and open to significant interpretation. We believe that this definition should be revised to limit it to realistic and defined cases, that do not go beyond the general concept of a public emergency. We suggest adding a health-specific definition of *'public health emergency'* as an exceptional situation negatively and suddenly affecting the health of the population of the Union, a Member State or part of it. Public health emergencies shall be defined as the occurrence or imminent threat of a life-threatening or otherwise serious hazard to health by biological, chemical, environmental, climate or an unknown origin, that poses a substantial risk to human health and wellbeing.

Furthermore, we propose to add a definition for *'exceptional need'*, which should be defined as a situation in which a relevant public authority, including a Union institution, body or agency, or a relevant national member state authority has exhausted all existing legal parameters in the pursuit of the appropriate data required to contribute to the mitigation of a public emergency.

Other definitions and concepts

Recitals 16, 18 and 84 refer to the term '*connected product'*, which is not sufficiently explained. More clarity is needed on what some of the hardware and interface criteria are that classify a device as a 'connected product' under the Act. This would allow for a more accurate demarcation between products regulated under the Data Act, and devices that are primarily designed to collect data for clinicians' use with a minimal external communication interface.

Furthermore, a definition of '*competing product and service'* relevant in the context of Business-to-Business data sharing obligations is needed, in order to further underpin principles on competition rules in the EU. Finally, the definition of a '*related service'* should be narrowed down to focus on the service essential for a product's 'basic function' rather than 'a function'.

3. Data accessibility and sharing obligations

a. Safety, security, and confidentiality concerns resulting from the interaction with existing sectoral legislation

By laying out data accessibility requirements, the Data Act adds a new layer of product regulatory requirements for products to be placed on the EU market. **The requirements as proposed in the Commission draft will lead to legal uncertainty for device manufacturers and regulators, pressures for the medical technology industry and subsequent impacts on future innovation in and for the EU market.** MedTech Europe thus calls for more legal clarity on the interaction of the requirements of the Data Act with the design of medical technologies, where existing sectoral legislation (MDR and IVDR) lay out product design requirements for medical technology manufacturers.

Safety concerns and potential impact on diagnosis and treatment of patients

Patient safety is of paramount importance to the medical technology sector. Therefore, MDR and IVDR, set out strict requirements for the medical technology manufacturers in terms of patient safety, security, protection against unauthorised access and availability of service. The main reason why a medical technology that generates or collects data qualifies as such under sectoral legislation is that it is intended to process, analyse, create, or modify medical information. As such, the software, which alters the representation of data for medical purposes would also qualify as medical device software to create readable and meaningful output for healthcare professionals and patients. In this regard, the validation and interpretation (through HCPs) of data may be part of the regulatory scrutiny under MDR and IVDR. **An obligation to provide access by systematically sharing *all* data collected by medical technologies outside this secure and regulated framework for interpretation may present unforeseen risks for patients' safety which must be carefully considered.**

Patients and even HCPs do not usually (and cannot be expected) to have insight into the functioning of the proprietary algorithms of medical technologies. Users, (especially patients), may not be able to interpret the raw data accurately, creating a risk of incorrect diagnosis or treatment decisions.

Security risks and impact on privacy and protection of health data

Making data from medical technologies directly available to users (e.g., via an open interface) could create real and unforeseen cybersecurity risks that are incompatible with the requirements under existing sectoral legislation and incompatible with the risk profile of medical technologies. MDR and IVDR require medical technologies to be designed with the utmost respect for information security (cybersecurity) and the confidentiality of device user/patient data.

The Data Act, however, obliges manufacturers to design their medical technologies in such a way as to make this highly sensitive user-generated data readily available, for further sharing with both the user and specified third parties. **Such requirements risk undermining manufacturers' sectoral obligations, and potentially the cybersecurity of user-generated data.** Furthermore, medical technology manufacturers do not traditionally know the identity of the patients who use their products. Therefore, secure pathways for patient identification must be clarified before mandating the transmission of data in order to enable the data flows mandated in the proposed Act.

Technical feasibility

The tight regulation under the MDR and IVDR mandates a range of product design requirements for medical technology manufacturers to demonstrate conformity, and for products to reach the EU market. Duplicated requirements and potentially contradictory obligations brought about by the Data Act **to make data easily and directly available to the user or specified third parties lead to uncertainty in this design process.**

Furthermore, there could be inherent limitations to the amount of data that can be managed in any given product and that can be transferred to an interface where it can be accessed. Transferring additional data points often requires significant modifications to the architecture and design of a product and could also come with impacts e.g., on battery depletion or computing power required for data hosting. This is of particular concern, e.g., when it comes to implantable devices, such as pacemakers for patients with cardiovascular diseases, where devices would have to be removed and replaced more often. This would lead to a potential impact in quality of life due to more frequent invasive surgeries and hospital stays for the patient, as well as higher related costs for healthcare systems.

Making all data directly accessible (including continuously or in real-time in a machine-readable format) would require significant processing power and hence come with significant concerns regarding early battery depletion, leading to (much earlier) device replacement (e.g., for implantable devices).

The potential need for re-certification and impact on device availability in the EU

If compliance with the Data Act requires design adjustments to the product design of medical technologies deemed as 'substantial modifications', it would also entail a likely need for a product to undergo an additional conformity assessment procedure, and re-certification to obtain the required CE-

marking. In this context, existing backlogs in the conformity assessment procedure of medical technology to be placed on the EU market would be exacerbated. This is likely to have further adverse impacts and healthcare systems in Europe, with disruptions of supply of medical technologies for hospitals and patients.

MedTech Europe thus strongly recommends that the new design requirements will not be applicable to products already placed on the market or put into service to alleviate some of the above-mentioned potential impact on availability of medical technology on the EU market.

Making additional data points available may create a possible impact on the functioning of the technology when this was not part of the original design. If a complex system of device data collection and monitoring is currently certified as a whole, it could require re-certification or even a new certification of legacy medical technologies under MDR/IVDR to comply with the Data Act provisions.

MedTech Europe calls on EU co-legislators to not apply the data accessibility and sharing provisions on data generated by the use of MDR/IVDR-regulated devices if it compromises the above-mentioned principles of safety, security and performance of medical technologies or protection of patient data required under existing EU legislation, namely the MDR, IVDR and GDPR.

b. Data sharing obligations to third parties & IP protection

MedTech Europe is concerned that the Data Act could have unintended and potentially detrimental consequences on a company's ability to protect critical IP assets. This could lead to a situation where IP and trade secrets' legal protection become the subject of a gradual erosion, where possible consequences include, for example, multiple disputes overloading national judicial systems, heavy burden of proof on the initial data holders, etc.

The inner workings of a product (or related services), such as medical technologies, are the result of substantial investment in research and development. Manufacturers need to ensure that proprietary information is protected as a trade secret to prevent third parties from using such information, for example, to develop competing products or services without consideration of the original investment. MedTech Europe believes that rules relating to Intellectual property rights (IPRs) in Europe play a significant role to ensure that medical technology companies remain incentivised to invest in research and development while new jobs are created, and healthcare delivery continues to improve for the benefit of European citizens and health systems.

Trade Secrets

With regards to trade secrets, the explanatory note of the Data Act states that the proposal does not affect existing rules in the area of IP (except the application of the *sui generis* right of the Database Directive). However, Article 4(1) allows users to access information that would fall under the scope of Directive (EU) 2016/943 (the "Trade Secrets Directive''). To that effect, the Data Act foresees that specific

necessary measures may be taken to preserve the confidentiality of trade secrets.[8] For the moment, it is unclear how those measures could look like nor whether they would be effective and sufficient.

The proposal states that the data holder and the user can agree on measures to preserve the confidentiality of the shared data, in particular in relation to third parties. The proposal also states that trade secrets shall only be disclosed to third parties to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party. Yet, it is unclear by which measures and how effectively any trade secrets will be protected in practice, particularly when the data holder and the user or third party failed to mutually agree on the necessary measures to preserve confidentiality. In particular, situations where the user could share the data with competitors, including non-European, would be problematic especially with no rules to govern neither compliance nor breach.
Moreover, there is a contradiction between Articles 5 and 6 versus Article 8(6): the latter suggests that there is no obligation to disclose trade secrets, whereas the other articles seem to indicate that under specific conditions, there can be an obligation for the data holder to share trade secrets.

As such, the draft essentially obliges disclosure of trade secrets and/or proprietary information to users, third parties and public bodies if necessary for the purposes pursued by them, and only loosely refers to 'necessary' or 'appropriate' measures to preserve confidentiality while the safeguards and remedies are disproportionately weak[9].

MedTech Europe recommends that trade secrets are clearly exempt from the scope of the final regulation, with full references to Directive (EU) 2016/943, which should take precedence.

Databases

With the introduction of the Directive 96/9/EC (the "Database Directive"), two protection schemes for databases in the EEA have been introduced, one of which is copyright - which may protect the structure of a database - and the second one is the *sui generis* database right. The latter is subject to the requirement of "substantial investment" (in any quantitative or qualitative matter) in obtaining, verifying, or presenting a database. The right protects also from extraction and re-utilisation of the content of a database (whole or substantial part or systematic, if non-substantial). with the overall goal of the Database Directive being to foster innovation and encourage investment in databases.

In connection with the user that owns, rents, or leases a product or receives a service, the Data Act proposes in Article 4 "*The right of users to access and use data generated by the use of products or related services*" and in Article 5 "*Right to share data with third parties*" where a user requests a data holder to do so. It further proposes in Article 35 the rights of users to access and use data from databases containing data obtained from or generated by the use of a product or a related service, is excluded from the protection available under the *sui generis* database right.

[8] Art. 4(3) Data Act proposal
[9] Art. 11(2) and (3)

Excluding the *sui generis* database right from application to databases containing data obtained from or generated by the use of a product or a related service, denies the protection of the substantial investments in these databases. In the field of connected medical technology, such databases are essential, including for purposes of regulatory compliance and patients' safety, and, because of the cost related to the data collection and storage in accordance with applicable requirements and at market value compensation for those involved (e.g., healthcare organisations), constitutes substantial investments for the medical technology manufacturers.

Therefore, rather than weakening the *sui generis* database right altogether, we suggest amending the proposal and **clarifying that it cannot be invoked to hinder the effective exercise of rights provided for in the Data Act, therefore ensuring the protection to the substantial investments.** It may also be necessary to further clarify what is meant by "substantial investment".

4. The interplay with other legislation

a. Interaction between the Data Act and the GDPR

We understand that the Data Act is designed to complement the existing right to protect personal data under the GDPR. However, MedTech Europe believes clarification is needed on the interplay between the Data Act and the GDPR, particularly on the terminology used in both regulations and the roles of the parties ('*data holder*'[10] vs '*data controller*[11]' and '*data processor*').
It is unclear who would classify as a 'data holder' as the value chains in healthcare settings are very complex. For example, if hospitals are considered data controllers, manufacturers would be data processors acting upon instructions of hospitals when it comes to the processing of personal data. This could mean that the Data Act would provide an access right from the patient directly to the medical technology manufacturer, which would conflict with the provision under the GDPR, where a medical technology manufacturer qualifies as a '*data processor*'. This issue is particularly relevant in the healthcare sector where the manufacturer of a product (i.e., the medical technology company) often does not have a direct relationship with the typical consumer (i.e., patient) but with intermediates like hospitals, or HCPs.

Medical technology manufacturers are not always the data holder and in control of the data. This goes not only for personal data but also for non-personal data generated by the use of a medical technology. In the latter case, if a HCP is deciding on the use but the device is worn by a patient, medical technology companies would be subject to strict confidentiality obligations and hence not be allowed, under their agreements with healthcare organisations, to make (non-personal) data directly available to patients.

Similarly, the 'user' as defined by the Data Act could be a healthcare organisation whereas the actual user of the technology are HCPs. It is unclear to what extent they are entitled to request access to data

10 Data Act, Art. 2 (6)
11 Data Act, Recitals 23 and 24

as provided by the Data Act if they are formally not the buyer of the technology but use it in the context of their work as HCP. MedTech Europe would therefore welcome a definition of data portability, consistent with the GDPR.

Patients often wear prescribed medical technologies with data only being accessible to HCPs. This is for example the case with implanted cardiac devices. In such instances, it needs to be clarified who is considered the 'user'.

MedTech Europe urges to have clear distinctions between *'data holder'*, *'user'*, and *'data recipient'*, and better alignment with the concepts of *'data controller'*, *'data processor' and 'data subject'* under GDPR.

b. The interplay with future legislation

It is fundamentally important to align interacting pieces of legislation to ensure legal certainty. **Thus, MedTech Europe calls for legal clarity and alignment with other legislation**, such as the proposed European Health Data Space (EHDS) Regulation[12], the Data Governance Act[13], the Artificial Intelligence Act[14], the Cyber Resilience Act[15] and NIS2 Directive[16], particularly with respect to terminology, concepts and definitions. In addition, we call for alignment with the Product Liability Directive[17, 18] (currently under revision), which already includes terminology, definitions and requirements covering various aspects of the proposed Act.

MedTech Europe supports the approach taken in the EHDS proposal, prioritising selected patient data to be made available in the electronic health records (EHR) of natural persons via secure ways to share this data. To the extent that raw data is of interest to professional users and patients, a similar '*phased*' approach under the Data Act would allow for broad stakeholder consultation and consider the '*value*' of data versus the complexity of making the data securely available in a common format. In this regard, it is important to note that so far, no common data standards for 'raw' data (as opposed to 'health' data, meaning interpreted data that provide clinical insight) have been or are being developed. It would be recommendable to focus on the EHDS, prioritising health data that are most of interest to patients and healthcare providers.

Data sharing with public sector bodies

In addition to data access and disclosure commitments, Chapter V of the Data Act mandates compulsory disclosures of data to public sector bodies (business-to-government or B2G data sharing) in cases of '*exceptional need*', such as public emergencies. Though public sector bodies authorised to

[12] European Health Data Space
[13] Data Governance Act
[14] Artificial Intelligence Act
[15] Cyber Resilience Act
[16] NIS2 Directive
[17] Product Liability Directive
[18] Product Liability Directive - Adapting liability rules to the digital age, circular economy and global value chains

compel access are required to comply with procedures set out by the Data Act, there is a need for further clarity on the terms of such data-sharing obligations.

MedTech Europe considers the definition of '*public emergency'* in Article 2(10) as too broad, which leaves room for interpretation. We, call on legislators to define a 'public emergency' as an exceptional situation negatively and suddenly affecting the health of the population of the Union, a Member State or part of it. A *'public health emergency'* shall be defined as the occurrence or imminent threat of a life-threatening or otherwise serious hazard to health by biological, chemical, environmental, climate or an unknown origin, that poses a substantial risk to human health and well-being. Furthermore, the definition should be narrowed in Art. 15, by providing more objective criteria for determining the type, the timeframe, and the magnitude of the actual or expected negative impact on the public.

To give sufficient guidance on those incidents, we suggest also provide for a definition of *'exceptional need'* under Article 2 on definitions. 'Exceptional need' should be described as a situation in which a relevant public authority, including a Union institution, body or agency, or a relevant national member state authority has exhausted all existing legal parameters in the pursuit of the appropriate data required to contribute to the mitigation of a public emergency.

Furthermore, we want to outline that the definition of 'public sector body' in Article 2(9) is defined very broadly and would cover all entities governed by public law and associations. This broad definition could potentially include mixed public-private partnerships and public research institutes. The final regulation should limit the definition to bodies in relation to the 'specific tasks in the public interest'.

Finally, it is of relevance that, according to Articles 19 and 21 of the proposed Act, public sector bodies are entitled to share data that they receive with individuals or organisations carrying out scientific research or analytics related to the purposes that led to the original request. This could result in public sector bodies which requested data in connection with a public health emergency transferring that data to third parties for research purposes that are not regulated, and under circumstances whereupon the data shared is not sufficiently protected.

We therefore want to stress the need for more clarity on the terms for B2G data sharing and reassurances that companies will not see their competitiveness unduly impacted by the sharing of such data, as well as adequate measures to protect commercially sensitive data (e.g., trade secrets, know-how).

6. Interoperability and Data Portability

Identifying and defining relevant interoperability standards will be essential for ensuring the implementation and enforcement of several provisions of the Data Act. MedTech Europe supports portability and interoperability requirements that allow users to switch between data processing service providers, especially to the extent that this may support the implementation of the future EHDS**. We**

wish to highlight that many international consensus standards and best practices already exist and should be further recognised in the Data Act itself or through Implementing Acts. Chapter VIII should be based on such existing standards and best practices and cooperation at the level of international and European standardisation organisations should be legally formalised.

We call for the further development of open interoperability specifications or European standards for interoperability for data processing services, which should build on international consensus interoperability standards that will prevent creating unnecessary hurdles to seamless international data flows. By the same token, MedTech Europe would like to highlight that European harmonised standards should be primarily used instead of key common specifications to accurately reflect the state of the art, particularly with respect to cybersecurity. EU policymakers should duly consider industry best practice in this regard or promote development of the same to allow seamless international data flows.

Regarding data portability, we want to underscore that any such strict obligations on this market should be carefully considered. Article 26(1) lays out the technical aspects of switching providers and mandates service providers to ensure that the customer, after switching to a service covering the same service type offered by a different provider of data processing services, enjoys functional equivalence in the use of the new service. However, the transfer of configuration parameters, security settings, access rights and access logs may amount to conveying detailed information about internal processes of a service provider, e.g., a company's know-how. In addition, the combination of easy switching and short-term customer contracts reduces any investment incentives for lasting improvements in data quality where data quality is dependent on service performance.

We, therefore, would like to stress that the obligation to have a maximum termination period of 30 days to transfer all data to a competing service provider is technically unfeasible and would considerably undermine the competitiveness of EU actors' cloud offerings. This could, in turn, have a cascading effect on the medical technology industry and we, therefore, recommend prolonging the indicated termination period to be defined and agreed between the parties to transfer data to other service providers. Rigid conditions would fail to reflect specific customer situations and transition periods should consider the level of complexity of the architecture, the array of services provided, and the volume of data processed.

7. International transfers

The proposed international data access and transfer requirements are at risk of imposing data localisation and resulting in non-EU jurisdictions implementing, as a counter-reaction, data localisation as well, which could lead to more data fragmentation and increases of infrastructure implementation costs. MedTech Europe recommends clarifying the terms '*access to data'* and '*transfer'* to provide more legal clarity and certainty.

8. Enforcement and application

In terms of reinforcement of the Data Act provisions, we want to highlight the potential for fragmentation in the interpretation and enforcement of the regulation. Article 31 mandates the EU Member States to establish one or more new authorities or rely on existing authorities responsible for the application and enforcement of the provision of the Regulation**. MedTech Europe is concerned that Member States would designate different authorities under the Data Act than the Data Protection Authorities or other competent authorities (e.g., in relation to the AI Act). Even though the Data Act refers to the need for cooperation, situations could arise where there are multiple authorities considered competent.** Possible divergent approaches could lead to serious compliance challenges for medical technology companies and would create further uncertainty with regards to the implementation of the provisions.

In addition, MedTech Europe encourages legislators to modify the entry into application of the requirements of the Data Act. The current 12 months period represents too short a timeframe for the medical technology industry to sufficiently adjust existing structures in order to comply with requirements. Therefore, **MedTech Europe suggests that legislators amend the date of application to 48-months**, to ensure that all relevant stakeholders can sufficiently adapt to the new and far-reaching requirements of the Data Act.

Furthermore, given that the proposed Data Act aims to introduce substantial changes to the legal framework covering the data-sharing contractual practices, it should provide for a sufficient timeframe to amend or re-negotiate pre-existing data-sharing agreements with third parties. Consequently, **MedTech Europe suggests allowing for certain "sunset clauses" with a specified grace period of an additional 12-months** to ensure a smooth and effective transition.

9. Conclusion

We believe that the success of the proposed Data Act will depend on clear rules that take into account sector-specific considerations, are aligned with existing legislation, and that will support individual rights, the confidentiality of business information, the upholding of IP rights and better access to technology innovation. MedTech Europe and our members look forward to closely collaborating with legislators and stakeholders to ensure that the Data Act protects the rights of European citizens and fosters innovation based on data-driven solutions.

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.

Contact: Verena Thaler, Manager Digital Health, v.thaler@medtecheurope.org