COCIR Feedback

Proposal for a European Data Act

Introduction

COCIR welcomes the opportunity to provide feedback to the European Commission's proposal for a European Data Act. Without a doubt, Data Act will play an important role in shaping Europe's digital future. The proposal aims mainly at creating a regulatory framework to ensure fairer value allocation from data and foster access to and use of data. It is important, however, that it maintains incentives to invest in ways of generating value through data and ensures consistency with the existing legislation, in particular the General Data Protection Regulation and Medical Device Regulation, which already include requirements covering various aspects of the proposed Data Act.

Recommendations

The Data Act is being followed by the European Health Data Space (EHDS) which specifically addresses the healthcare market and its needs for electronic health data. However, very broad formulation of the essential elements in the Data Act, which will serve as the foundation for EHDS requires further fine-tuning to ensure legal clarity and consistency, in particular with regards to the following:

I. Clear definitions and concepts

Without a doubt, healthcare is a unique sector. One of many unique characteristics is that users of medical devices are usually clinicians rather than patients. This alone creates confusion what kind of data could be requested by clinicians, operating the medical device to perform clinical duties, and the patients, whose data have been collected and/or stored on the medical device. This calls for more clarity on the scope of data to be provided by data holders, establishing reasonable limits of information that the user may have the rights to request, and the data holder is obliged to provide in each instance.

The proposed definition of 'data' is very broad and includes both personal and non-personal data. It creates, however, an exception for information derived or inferred from this data. It is therefore not clear how the 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. In this respect, 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. It should not include data generated without any action by the user as such data may be subject to trade secrets and intellectual property rights.

Furthermore, the distinction between data holder, user, and data recipient should be better clarified as the (IoT) value chains are much more complex, e.g., the device manufacturer may not be the data holder and in control of data (also considering clinicians and patients).

II. Interplay with the GDPR

The proposed Data Act is not sufficiently clear on the differentiation between data controller and data processor. This distinction should be made, and obligations clarified, in line with the GDPR.

Also, to ensure that the Data Act aligns well with GDPR, we believe additional clarity is needed on the data holder concept. The description of a data holder in Recital 24 equates the data holder to a data controller whereas the definition of the same concept in Article 2(6) considers that for non-personal data any entity that has the "*technical ability to provide the data*" should be considered the data holder: this double standard is not justified and lead to inconsistency between the GDPR and the Data Act. Therefore, the same criteria should apply to personal and non-personal data when it comes to setting the entity obligated to share the data with users and data recipients.

The territorial application of the proposed Data Act should be further clarified, as to how it will interact with the territorial jurisdiction of other regulations, including e.g., the GDPR, MDR, e-Privacy Directive and any future relevant legislation.

There are already significant legal and practical concerns regarding when a dataset could be considered sufficiently 'anonymous' or 'non-personal' due to the lack of clarity/common understanding of these concepts across the EU.

Guidelines at EU level are needed to create more consistency and clarity on the concepts of personal/non-personal data and anonymization to ensure legal certainty for stakeholders as to what the implications of the Data Act vis-à-vis different datasets could be.

III. Incentives for investment fostering

The proposed obligation to share data may undermine market dynamics if not accompanied with clear and robust safeguards for data holders. The current proposal does not offer any clear mechanisms of the commercial rights protection for the manufacturer should their rights be breached by the user or the third party to which the data is transferred upon the request of the user.

While the transparency or access to large sets of data held by few companies may increase competition and innovation on the data market, for data sharing in specific sectors like medical and health devices, the likelihood of collusion between competition may increase and lead to competition concerns. In addition, this may discourage mid-sized companies to invest in expanding technology if they are at risk of having to share that what they have built up as not only IP and trade secrets are covered in the data, but also valuable know-how companies have invested in.

Trade secrets should be fully protected, data considered as trade secret should remain outside the scope as this is instrumental for incentivising investments and innovation regarding generation and processing of data. In view of that, the protection should not only cover trade secrets but also provide for measures against the potential "reverse-engineering" and obtaining trade secrets out of (e.g., machine) data that by themselves (i.e., before being analysed or reverse-engineered) do not contain trade secrets.

Recital 17 states that data as generated by a product fall within the scope of the data sharing obligations, but that data derived and calculated from it using software (calculations) falls outside the scope, because intellectual property rights may rest on that software.

However, this delineation is not reflected in the articles themselves. This will lead to ambiguity in the interpretation of the articles. Uncertainty contributes to problems in the implementation of the law and can lead to fragmentation in the EU. Therefore, all key concepts must be included in Article 2, and the scope of the obligations must be articulated clearly in other related articles to ensure unanimous application of the Data Act across the EU member states.

The following points are also of concern:

- Article 4.6 of the proposal forbids the data holder to use data generated by the use of the product or related service in a way that would undermine the commercial position of the user. It should be clarified what is meant by 'undermine commercial position of the user'.

- When it comes to sharing of data with third parties, the proposed provision of Article 5.8 regarding the disclosure of trade secrets is formulated too broadly and offers insufficient remedies to the data holder to prove that the user or third party has used trade secrets beyond the scope of confidentiality arrangements as the harm to the data holder is done at the moment the data is shared. Trade secrets should be fully protected, and data considered as trade secret should remain outside the scope to foster investments and innovation regarding generation and processing of data.

- The proposed provision of Art 6.2 (e) raises the concerns as to how will the data holder whose information has been shared demonstrate that a third party developing a competing product uses their information. This should be further clarified and the term 'competing product' should be defined as this may hamper innovation

The current formulation of the Data Act is focused on empowering the user, which is the right thing to aim for. However, the proposal pays little if any attention to the motivation of the manufacturers to invest into data generation, which is a source of innovation and economic progress, the ultimate driver of growth in wellbeing. COCIR would welcome elaboration of acceptable principles how generators of the data could participate in the additionally generated profits if their generated data is used to develop new products or services that compete with the products and related services that generated the data, not only make the data available and transfer it to third parties upon the request of the user.

IV. Requirements, and protection in the context of B2G data sharing

Regarding obligatory B2G data sharing, the proposal raises many practical concerns, such as insufficient guarantees from public bodies to protect the data holder's data should it be requested following Articles 14 and 18.

Not only it is important to ensure that Data Act does not become an instrument of unauthorised access to sensitive data in the name of public interest, but the definition of public emergency in Article 2 should also be revised as the currently proposed wording may be interpreted differently across the EU member states, following different levels of tolerance for similar events or situations. In addition, the expansion of conditions for obligatory data sharing beyond public emergencies as it is currently proposed in Article 15 is worrying because it may potentially depend on political interests rather than objective grounds.

The extension of "B2G" to "B2G2RS" data sharing should be limited to defined cases where the public interest considerations clearly outweigh (such as for public emergencies) and to

specific recognised and publicly funded research institutions. In addition, exclusion of micro small and medium enterprises from obligatory data sharing obligations under Articles 7 and 14 does not seem justified.

Another important aspect to comment is that while it is declared that the regulation intends to prevent abuse of contractual imbalances that hinder fair data sharing, the proposed means go beyond the intentions and pose potential risks of unfair behaviour and limitations in trust development among stakeholders. COCIR strongly believes that full exclusion of small and micro companies from B2B and B2C data sharing in Article 7 undermines the foundations for building trust both within the industry and with consumers. Moreover, in theory it may work against the interests of the society should the critical information be held in the hands of the most innovative SMEs.

In combination with the exclusion from B2G sharing obligations and imposing caps on compensation for granting access to data, rather FRAND terms should apply equally to SMEs as well. Cost-basis compensation may otherwise require disclosure of company's sensitive data and is deemed disproportionate.

V. International access to and transfers of non-personal data

Proposed restrictions to international transfers of non-personal data (especially on non-personal data as currently proposed in the Data Act) may lead to unacceptable limitations for business development as well as stable and secure business operations, given the international nature of mature companies in the healthcare sector. While protection of personal data is a fundamental right enshrined in the Charter of the Fundamental Rights of the EU and so must be protected, this is not the case of non-personal data which would be mainly business data. There should be clarity as to the reasons for granting the same level of protection to non-personal data as to personal data under the GDPR. Moreover, same concerns may potentially drive SMEs outside the EU as SMEs are in crucial need of the solid benefits brought by international data transfers such as cost effectiveness, choice of the best suited data sharing infrastructure and secure and resilient operations.

VI. Harmonised implementation and enforcement

COCIR would also like to raise concerns about the risk of variations in national implementations of the Data Act. Better integration and harmonisation of the structure and processes of Regulation implementation and enforcement on national level would be expected than it is currently proposed in Article 31 (Competent authorities). For instance, the Data Act could institute a pan-European supervisory authority or a one-stop-mechanism and clarify how responsibilities will be allocated between data protection authorities and sectoral regulators when it comes to sharing mixed data sets within or between specific sectors.

Furthermore, some practical issues, such as limitations in information access in different countries if only one language (Article 10, Dispute settlement) is used for decisions on disputes should be addressed explicitly so that to avoid continuity of fragmentation across business experiences across different EU Member States.

VII. Interoperability

Finally, the proposed provisions on interoperability should refer to the existing global interoperability standards and give preference to these internationally recognised interoperability standards. In particular, there should be a link to all relevant European and

international standards development organizations (SDOs) of all sorts, including industry consortia, and not only to the legally recognized ESOs (CEN, CENELEC, ETSI) or their global equivalents (ISO, IEC, ITU). This must be organized with due stakeholder engagement, in particular with industry. An important goal would be to align on shared views on the need for standards as input for SDOs, who could then base their own priority setting on better and more homogeneous market demand insights.

VIII. Interplay with the medical device legislation

Requirement for data 'accessibility-by-design' raises the question of the interplay with the provisions of the Medical Device Regulation as it may add an additional layer of product design requirements to medical devices, already strongly regulated.

The obligation to share data under the Data Act should in no way compromise the safety, security and performance of medical devices required under the EU legislation, in particular the Medical Device Regulation and GDPR.

IX. Sufficient transition period

The proposed transition period of 12 months should be extended to at least 48 months to allow for the necessary adjustments to be made by all the participants to the data ecosystem in scope of this proposal.

Conclusions

COCIR members take their responsibility towards end-users, especially patients, very seriously. COCIR is a strong advocate of a targeted regulation for digital data. Therefore, we welcome the efforts of the European Data Act to address multiple important aspects for businesses and consumers. However, there are some critical areas for improvement in the Data Act before the needed level of clarity and fairness in regulating products and services under the newly emerging legislative framework is achieved.

We are looking forward to engaging with the EU institutions in the upcoming legislative process, together with our technical experts.