Alliance for Internet of Things Innovation

Brussels, 14 June 2022

AIOTI Views on the Data Act

Clarifying scope of B2B data sharing provisions

In AIOTI's view the "data" covered by the scope of the Regulation seems to be inconsistent throughout the legal text. Articles 2 and 3 can be understood as covering data generated by an IoT/connected product or related services . Chapters II and III, and Chapter VI, however, appear to entail a broad range of data. The lack of clarity on the scope of data covered and the players implicated complicates how the exercise of new user rights would work in practice, particularly for B2B scenarios. In this context, clarification on the definition of 'data holder', 'data user' and "operators of data spaces" that operate in complex B2B environments of "products" and "related services" would be helpful. Along the B2B value chain an enterprise can thus be both the data holder and the data user under the Regulation. This would cause legal uncertainty as to the obligations of the provisions, and to whom they ultimately apply, for instance when acting as data processors from a GDPR perspective and when processing mixed datasets. Therefore, the definition of data holder in Article 2(6) should use the same criteria for personal and non-personal data, and operators of data spaces should be defined as operators of Common European data spaces.

In this context the exact scope of the Data Act and its differentiation from Regulation 2016/679 seems unclear as any obligation of the data holder under the Data Act will require to link all data to an identifier in order to fullfill an user´s request, therefore potentially creating personal data. Even where a user is an enterprise or other legal person Regulation 2106/679 should apply when natural persons acting on behalf and/or with power of attorney remain generally identifiable and therefore should be considered data subjects under Regulation 2016/679.

Regarding the provisions on contractual fairness, AIOTI is a proponent of contractual freedom. The provisions in the Data should not impede the ability of companies to conduct business according to basic contractual freedom rules. Our members should be able to decide and to negotiate themselves to what extent and under which conditions they will share their data with third parties. If there are any imbalances or gaps, they should be addressed by EU competition law or sector specific legislation.

Clarifying scope of B2G data sharing provisions

Only in the case of a duly justified exceptional need, AIOTI would support the provision of data for government tasks. However, this must be reduced to a few, particularly justified exceptional cases. The experiences of the past years have shown that crisis situations can last for a long time. This results in a large room for manoeuvre for the public authorities, which must be limited. As a result, there should be no state of permanent data access. Companies and public bodies need more legal certainty in this regard.

In order to achieve this goal, it should be avoided that the vague legal term "exceptional necessity" used in Art. 15 is concretised with further vague legal terms "public emergency" and "other exceptional situations". The aforementioned legal terms open up a wide range of scenarios, many of which go beyond the willingness of companies to provide their data. For this reason, there is a need for a clearer definition of the extent to which companies must provide data to public bodies in terms of time and content. Public bodies should be given clearer guidelines, especially with regard to the very broadly interpretable tasks to be fulfilled in the public interest as mentioned in Art 15 lit. c). It is also unclear how data may be passed on or used and to what extent sufficient protection of sensitive data is to be guaranteed. Protective measures for companies are therefore urgently needed.

In any case, the companies need adequate compensation and suitable conditions for efficient provision. The collection and transmission of data is associated with a high administrative effort and costs for the companies, which is not or only partially compensated in the envisaged draft.

Avoiding vendor lock-in while striking the right balance

AIOTI welcomes the objective of Chapter 6 to support data portability and to prevent anti-competitive behaviours by locking in cloud users. Cloud switching and data portability is well established in the EU and is increasingly expected from cloud users. Best practices in cloud increasingly support hybrid and multi-cloud models, which are environments designed to maximise choice and portability, and to switch easily between cloud service providers.

The provisions on cloud switching and portability in the Data Act should keep the right balance between clients' and providers' operational responsibilities. As such, the provisions must take into account the practical complexities of such activities in a cloud environment. Switching in a B2B cloud environment is not as simple as, for example, an end-user switching mobile phone operators. In our view, the Data Act should be a balancing act between customer choice, competition and the technical aspects. Particularly Articles 26.1 and 2(14) that contain the obligation to ensure "functional equivalence" should entail a reasonable level of cooperation between providers, and support from the customer, who should be able to define the minimum level of functionality referred to in Article 2(14). This could help further define the notion of "functional equivalence".

Exclusion of derived data, clearly specified in the definition

Recital (17) distinguishes clearly the data generated by the use of the product - subject to the Chapters II and III of the data act - and derivative data or in other words the "data resulting from any software process that calculates derivative data from such data" The latter falling outside the scope of such data act provisions.

We recommend to introduce this terminology as a general distinction into the main-definition part – in particular for the purpose of specifying the obligations for the data holder under Article 3.

Alliance for Internet of Things Innovation AISBL | Avenue Louise 65, B-1050 Brussels, Belgium | RPM Brussels 0663895516
Contact: info@aioti.eu | T: +32 (0)2 535 77 92 | EU Transparency Register: 380738729287-22

Promote the cooperation between providers during switching

Our members believe that efficient, smooth and workable switching of data processing services requires the cooperation between the three parties that are (1) the customer, (2) the original service provider, and (3) the new service provider, based on their specific obligations and relevant responsibilities.

Only such collaboration between providers and customers would ensure t removal of barriers but also ensure a switching between same services type Therefore, we recommend focusing on assistance of the original data processing service provider with the aim to complete the switching, subject to the cooperation of the customer and the new service provider. This will more adequately reflect the roles and responsibilities of the parties in practice.

Align data sharing obligations with industrial reality

The current definition of related services and recitals of the text are aiming to exclude products such as smartphones, tablets etc. and their related services. However, there is an increasing convergence of such consumer devices applications with other IoT devices applications which do not constitute core functions of these second type of devices. In such scenarios, the regulatory landscape would be impractical if manufacturers are faced with the risk that any smartphone application when broad-in into an IoT scenario will suddenly qualify as "related service" even when the user is only aiming at using such application through smartphones.

Therefore, we would recommend to narrow the scope to those related services to those that are indispensable for the "core functions" of "products" and are generated by the use of sensors.

Clarify data sharing requirements on design, manufacturing and mandatory elements to contracts

Concerning the obligations on the design and manufacturing of products and related services in Article 3 of the proposal we would recommend to further clarify this obligation. For instance, specifying the meaning of "easily" and "appropriate" concerning the accessibility of the user to its data in Article 3-1, would facilitate the applicability of the requirements.

Secondly, we believe that specifying the volume of data to be generated by the use of the product would be counterproductive to the objectives of the text and add little value to the market. This for the following reason:

(1) It will be hard to quantify the volume of data to be generated in advance – and thus this information may be inaccurate;

(2) Even if accurate, knowing the volume of the data adds little value to the user;

(3) Such requirement is going beyond what is required under the GDPR for personal data;

(4) Such requirement adds administrative burden and legal uncertainty to the data holder, in case the volume estimate proves not to be accurate.

Alliance for Internet of Things Innovation AISBL | Avenue Louise 65, B-1050 Brussels, Belgium | RPM Brussels 0663895516
Contact: info@aioti.eu | T: +32 (0)2 535 77 92 | EU Transparency Register: 380738729287-22

Promoting cross-border data flows

We believe that regulation should strive to solve conflict of laws, not institute them, and that conflict of laws should be solved through multilateral government talks, not by one government regime imposing unilateral requirements on a specific sector. In AIOTI's view, international data flows are indispensable for European companies' competitiveness, as they operate in a connected environment that goes beyond the EU's borders.

Furthermore, personal data and non-personal data are different in nature, requirements and legal mechanisms and these differences should be accounted for in policies covering international transfer of data and government access to data. Also, GDPR clearly sets forth the conditions for lawful cross-border transfers and thereby creates certainty, whereas Recital 77 contains a reference to a broad list of rules applicable throughout Europe and in the Member States and therefore creates ambiguity.

Also, data transfer policies should be tailored to reflect a workable balance of addressing identified risk and allocating responsibility to those entities that are best able to assess whether the data at issue is subject to any relevant transfer restrictions.

We would also encourage the Commission to solve issues around foreign authorities' access to data through multilateral governmental discussions rather than by imposing regulatory requirements on a specific sector. If such consensus cannot be found, we recommend that before contemplating regulatory intervention, the Commission considers the adoption of voluntary guidelines to serve as a robust set of best practices laying a future-proof standard on law enforcement requests for data for data controllers and processors alike. Any guidelines by the European Innovation Board should be developed in full and transparent consultation with industry. In addition, any opinions given by competent bodies or authorities as to the conditions of transfers should be detailed, robust and timely.

Ensuring coherence with the EU regulatory landscape

AIOTI stresses the need to stay consistent with current and incoming legislation. As indicated above already, the notion of the interaction between data holder under the Data Act needs to be consistent with the notion of data controller under the GDPR. The European Commission could also make the interaction of the Data Act with the AI Act under negotiation more explicit. Moreover, ensuring consistency with the upcoming ePrivacy Regulation, the Digital Markets Act, the Digital Services Act, the Free flow of Non-Personal Data Regulation but also the upcoming proposal on establishing a European Health Data Space, will also be key to ensuring coherence and legal certainty for companies.

There should be no additional bureaucracy

The proposed Data Act lays down new conditions in relation to the functionalities of products, which is a limitation of entrepreneurial freedom and an additional burden for product innovation. There should be in our view no bureaucratic requirements (e.g. information obligations of the manufacturer of products).

Alliance for Internet of Things Innovation AISBL | Avenue Louise 65, B-1050 Brussels, Belgium | RPM Brussels 0663895516
Contact: info@aioti.eu | T: +32 (0)2 535 77 92 | EU Transparency Register: 380738729287-22

Sufficient protection of intellectual property rights and trade secrets

The intellectual property rights and trade secrets of our companies are not properly protected by the Data Act as proposed by the European Commission. We believe that these rights must be better protected against unauthorised access and use.

Standardisation should be inclusive and industry-driven

While AIOTI supports the objective of Chapter 8 to support standardisation efforts in the field of interoperability to drive the objectives of the Data Act, the process to develop open interoperability specifications and European standards on interoperability should be based on participatory and industry-driven practices. Moreover, the European Commission should closely cooperate with European Standards Organizations and International Standards Organizations in developing these.

Ensure protection for certain databases and confidential business data

AIOTI believes that the text as proposed in the Data Act is an appropriate balance, as it aims at ensuring IP protection for certain datasets, while clarifying the scope and applicability of the sui generis right. In particular, recital 84 clarifies that the Act doesn't change the protection afforded by the Database Directive by stating that the users can access and use "*data in databases obtained or generated by means of physical components, such as sensors, of a connected product and a related service [..] where such databases do not qualify for the sui generis right*". We believe that in order to ensure clarity on the IP protection and to avoid confusion in implementing the Regulation, Article 35 should be further aligned with recital 84 by specifying that "*the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service, **unless such databases qualify for the sui generis right.***"

Besides, we would recommend to expand the scope of protection to cover not only trade secrets, but also confidential business data. In most cases these two categories will overlap. However, certain confidential business data may not qualify as trade secrets but may nevertheless warrant protection under this Regulation because of the possibility that they could reveal trade secrets. This is the case for specific datasets that individually are not qualifying as trade secrets, but when cross-referenced would reveal trade secrets.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT Innovation in Europe, bringing together small and large companies, start-ups and scale-ups, academia, policy makers and end-users and representatives of society in an end-to-end approach. We work with partners in a global context. We strive to leverage, share and promote best practices in the IoT ecosystems, be a one-stop point of information on all relevant aspects of IoT Innovation to its members while proactively addressing key issues and roadblocks for economic growth, acceptance and adoption of IoT Innovation in society.

AIOTI's contribution goes beyond technology and addresses horizontal elements across application domains, such as matchmaking and stimulating cooperation in IoT ecosystems, creating joint research roadmaps, driving convergence of standards and interoperability and defining policies. We also put them in practice in vertical application domains with societal and economic relevance.

Alliance for Internet of Things Innovation AISBL | Avenue Louise 65, B-1050 Brussels, Belgium | RPM Brussels 0663895516
Contact: info@aioti.eu | T: +32 (0)2 535 77 92 | EU Transparency Register: 380738729287-22