Alliance for Internet of Things Innovation

Brussels, 29 January 2021

AIOTI Response to the public consultation on the Data Governance Act

Overall:

- For most IoT ecosystems, in order to support addressing societal challenges having trusted open and dynamic data readily available as core facility, it is prerequisite to have such data and derived data and being able to use it, to add to such ecosystems and understand how to share and otherwise being able to use such data and derived data.
- AIOTI therefore supports the EU Data Strategy for having a more comprehensive approach to data sharing, data governance, ownership, access and data spaces.
- AIOTI also support Data Governance Act main objectives of open data sharing, improved data sharing and data altruism, common EU data spaces, ensuring legal certainty which will drive sharing and availability of data, as well as communicating best practice in data sharing.

Main principles:

- A major objective should be that end users can trust the data they have access to, and that the data has accompanying metadata concerning its sources thereby providing information about its provenance.
- Data sharing should rely on interoperability and other standards (taking into account the (implementation of) the European Interoperability Framework and also international ones) and portability to avoid any vendor lock-in. Data flows in B2B domain should be based on contractual freedom in data sharing.
- Data and data spaces are very relevant to make IoT ecosystems work. AIOTI already provided a separate set of comments about Common European Data Spaces.[1]
- IPR, commercial confidentiality and legitimate business interests needs to be properly protected from unlawful access.
- Access to data for researchers is important and needs to be open, while objectives of use must be clearly expressed.
- Controlled access to data should be based on clear cybersecurity requirements.
- The role of the public sector should be to provide a role model in providing access to data, as well as to guaranteeing access to data.
- Potential anti-competitive behaviours by open data users (including users that derive data from such open data sets and data sources) that will be tackled with Digital Services/Market Act should be carefully balanced with incentives from the European Data strategy and Data Governance Act.
- The process of requesting the re-use of public sector data introduced by the mechanism under the Regulation must be simple, time-efficient, and not require companies to do time-consuming investigate work, especially for SMEs. This mechanism should not become a bottleneck for companies to request such data under the Regulation.

[1] AIOTI input to the public consultation on Data Sharing in the EU - Common European Data Spaces

Potential obstacles:

- Protection of privacy: can still be a big hurdle, more guidance and perhaps regulation on how to anonymise data is needed from European Data Protection Board (EDPB) as well as more use of industry standards, in particular for mixed data sets. Furthermore, except for the current interim period regarding the UK, it is not yet clear how data transfers with the UK and US will continue and how adequacy will be achieved.
- National bodies will decide whether to grant or re-fuse access to sensitive public sector data There are concerns that this may lead to divergent approaches across the EC with resultant fragmentation of the EU common data space.
- Secure interoperability is not standardized for existing interfaces used by IoT devices which Is a pre-requisite for data governance.

More specific provisions:

- With regard to the re-use of public sector data, it is important to clarify whether data marked as sensitive be used only on request.
- It remains unclear which is the scope and who are the addressees of this regulation. In industry, there are plenty of functioning data-based business models based upon contractual arrangements and model clauses. For these settings, an additional layer of compliance would be counterproductive and create uncertainty. Chapter III of the Regulation should, therefore, not be applicable to data sharing in the context of industry arrangements or services. There is an imbalance between a kind of „voluntary" approach and quite strict penalties („cessation"). In Recital 22, some explanations are provided and some exceptions are listed, but a clear set of criteria is missing.
- It is of utmost importance to clarify the scope and definition, the criteria which are putting data services in the scope of the Regulation and the notification/enforcement procedure (or state clearly that this is a „voluntary" notification, but then it is considered as a kind of label).
- It is important to clarify if services falling within the scope of the Regulation these exist alongside current data sharing models.
- It is also not clear if when notifying an intermediation service at national level, must a data intermediary also notify the underlying technologies it uses to enable its services?
- It must be clearly acknowledged that contractual arrangements are a valid alternative to this model
- The concept of increasing trust by setting minimal requirements for „data intermediaries" is purposeful and most of the requirements reflect what should be expected from this kind of service.
- It is important to clarify cybersecurity requirements to data and related communication, devices and services.
- It should be clear what happens and what companies must do with data they already have and that falls out of the scope of the draft regulation.
- It is important to have a better understanding of the foreseen "European Data Innovation Board", will it be open and inclusive to all types of industry stakeholders? What will be its role and tasks concretely? On standardization it should coordinate with all relevant Standardization Bodies at international and European level.