Alliance for IoT and Edge Computing Innovation

Brussels, 8 November 2022

AIOTI views on the Data Act

Introduction

The Alliance for IoT and Edge Computing Innovation welcomes the Data Act and its particular focus on IoT related data. We also appreciate the effort made by the European Parliament and by the Council to intervene on the Act to further strengthen its scope and vision.

It is the opinion of our members that some additional input might be required to clarify specific concepts on B2B data sharing, on cloud switching, on international transfers and government access, on interoperability, and on implementation and enforcement.

Chapters II and III - B2B data sharing

We welcome the Data Act's B2B data sharing mechanisms, as we believe these have the potential to ease additional data flows, which will help to develop European competitiveness and an innovative data driven economy.

However, we think that additional clarity is needed on several elements, such as **the concept of a data holder or the scope of the data** to be shared and accessed by the user.

In general, setting **different standards to define data holders for personal and non-personal data is neither appropriate nor justified**. Therefore, Recital 24, which equates *personal* data holder to a data controller, and Article 2(6) which considers as a *non-personal* data holder any entity that has the technical ability to make data available, should use the same criteria. This will foster trust in data flows and technology and allow cloud vendors to implement the right safeguards to ensure that clients have control over their data (as required by Recital 78). Consistent with the above, Recital 21 should be clarified to ensure that cloud storage providers, who never act as data controllers, would also not function as data holders.

The current text provides for **"necessary measures" to protect trade secrets and confidential business data that could lead to the revelation of trade secrets**. Especially, in relation to third parties. In practice, this will lead to difficulties, especially in the case of medium-sized companies, which may end with the loss of valuable information and create new uncertainties and business risks for companies engaging in the data economy.

In fact, the Section 2 of the Explanatory memorandum of the proposal states: "*The protection of confidential business data and trade secrets is an important aspect of the well-functioning of the internal market, as is the case for other contexts in which services are exchanged and goods are traded*" by mentioning both the term "*confidential business data*" and "*trade secrets*" and not only the notion of trade secret.

It is true that in most cases these two categories will overlap. This being said, certain confidential business data may not qualify as trade secrets but may nevertheless warrant protection for instance when datasets that do not qualify as a trade secret individually, but when cross-referenced, would reveal trade secrets.

We would also point out that, in the EU, mechanical engineering industry is characterized by medium-sized companies. The requirements of the Data Act represent an unproportionate burden for the sector, but also in other sectors **SMEs** will face difficulties to cope with the additional burden, sometimes unnecessary, and to protect their know-how.

Finally, we would note that data space initiatives and data sharing models are launched, which are not only about technical interoperability, but also provide for data governance models, adapted in detail to the needs of a sector or a business ecosystem. One example would be Manufacturing-X which aims at creating a common data space for manufacturing. This will enable the easy and swift set-up of data exchange mechanisms by reducing the legal and technical transaction costs, whilst creating trust in the lawful use of data. There is the risk that the horizontal provisions of the Data Act are constraining the potentials of these data space arrangements.

In view of all the above, we suggest the following amendments:

In recital 21 - remove only the following sentence: ***~~"The server may be the manufacturer's own local server capacity or that of a third party or a cloud service provider who functions as data holder.~~"***

Article 2(1)-'data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording. ***For the purposes of this Act, data should not include information derived or inferred from this data.***

Article 2(6) - 'data holder' means a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control ***~~of the technical design~~*** *of the product* ***at the time the data is generated by the usage ~~and related services~~****, the ability, to make available certain data.*

Article 3(1)- Products shall be designed and manufactured, and related services shall be provided, in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user, ***in so far that it is technically and commercially feasible.***

(a) The European Commission shall provide further guidance on the technical and commercial processes by which the data would be deemed easily, securely and directly accessible by the user.

Article 3(2) - Before concluding a contract for the purchase, rent or lease of a product or a related service, at least the following information shall be provided to the user, in a clear and comprehensible format:

(b) *(a) the nature* ***~~and volume~~*** *of the data likely to be generated by the use of the product or related service;*

Article 4(3) - Trade secrets ***and confidential business data*** *shall only be disclosed provided that all specific necessary measures are taken to preserve the confidentiality of trade secrets in particular with respect to third parties. The data holder and the user can agree measures to preserve the confidentiality of the shared data, in particular in relation to third parties.* ***Necessary measures may include strict and restrictive technical requirements to ensure the confidentiality of trade secrets.***

Article 5(10-New) - Trade secrets shall not be disclosed to third parties without consent by the data holder

Art. 5(11-New) - The data should contain a provision which ensures that sectorial B2B-data spaces which are based upon voluntary multisided agreements are not constrained and can provide for tailor-made data sharing agreements.

Art. 7(1) - The obligations of this Chapter shall not apply to data generated by the use of products manufactured or related services provided by enterprises that qualify as ***~~micro or small enterprises~~ SMEs****, as defined in Article 2 of the Annex to Recommendation 2003/361/EC, provided those enterprises do not have partner enterprises or linked enterprises as defined in Article 3 of the Annex to Recommendation 2003/361/EC which do not qualify as* ***~~micro or small enterprises~~ an SME****.*

Chapter VI - Cloud switching

In recent years, the strong growth of cloud computing has transformed traditional models of computing. When fully utilized, it enables levels of scalability, flexibility, and choice that cannot be readily matched using a traditional on-premises IT stack. However, enterprises have been held back from migrating certain complex and sensitive workloads to the cloud due to interoperability, portability, security, and regulatory concerns.

Under a hybrid cloud model, workloads are deployed on a combination of private cloud and public cloud, often in conjunction with a traditional on-premises stack. This allows an enterprise to keep critical applications or sensitive data on-premises while reducing costs and enhancing efficiency by migrating other workloads to private or public clouds.

Multi-cloud architectures involve the use of cloud computing and storage services supplied by multiple providers to eliminate reliance on any single cloud provider (a mono-cloud approach). This enhances business continuity and security and is particularly valued for mission-critical workloads and customers in sensitive sectors such as banks and governments. A typical multi-cloud implementation utilizes two or more public clouds as well as multiple private clouds in a heterogeneous architecture.

The Data Act requirements on Cloud switching should be targeted at avoiding vendor lock-in, while keeping the right balance between clients' and providers' operational responsibilities. These provisions must account for the practical and technical complexity of moving workloads while preserving customers' needs to be supported in their transitions, and in general, strike the right balance between customer choice, competition and technical aspects.

The other elements of concern we have identified are as follows:

1- **Fixed term contracts** - Article 23.1(a) provides that the customer may at any time terminate the contract with a *maximum* notice period of 30 days. This provision, read in conjunction with Article 25, seems to end the well-established practice of fixed term contracts, which feature lower prices and enable both customers and providers to manage and plan their costs, revenues and investments. The benefits of such contracts are hence shared by cloud providers and their customers alike. Customers can deploy cloud solutions at a lower cost, and cloud providers can predict budgets and invest funds into innovation, R&D, compensation of employees, etc. An absolute right to terminate cloud contracts at any time would undermine parties' decision to enter into fixed term contracts, resulting in increased prices for customers, and fewer options for cloud providers to invest in innovative products and services.

2- The timelines set by Chapter VI to switch from one provider to another also need to be re-examined. To allow for a workable, stable and smooth migration, customers should provide termination notices a minimum of 30 days before the switching process can start, to allow the incumbent provider to prepare the switching process. Only at the end of the switching process should the contract be terminated (contrary to the current wording of Article 23.1(a)). Also, if a provider can prove that limited timelines for a migration process are "technically unfeasible", it is in the interest of service and business continuity that this process should be prolonged for as long as necessary to become technically feasible to complete the migration, and not only for 6 months. (Art. 24.2).

The following amendments would address the above considerations:

> *Article 23.1(a) terminating, after a* ***~~maximum~~ minimum*** *notice period of 30 calendar days* ***or any other mutually agreed upon and reasonable under the circumstances timeframe****, the contractual agreement of the service,* ***being understood that termination charges shall not be considered an obstacle under this provision.***
>
> *Art. 24.2 Where the mandatory transition period as defined in paragraph 1, points (a) and (c) of this Article is technically unfeasible* ***or unreasonable****, the provider of data processing services shall notify the customer within 7 working days after the switching request has been made, duly motivating the technical unfeasibility with a detailed report and indicating an alternative transition period,* ***~~which may not exceed 6 months~~****. In accordance with paragraph 1 of this Article,* ***~~full~~*** *service continuity shall be ensured throughout the alternative transition period against reduced charges, referred to in Article 25(2).*

3 - The obligation for a Cloud service provider to ensure **service continuity** in Art. 24.1(a)(2). Even in traditional outsourcing contracts, which are subject to lengthy negotiations, clients/users and providers agree on specific service level agreements that providers must comply with during the termination assistance phase, where providers help clients to migrate their workloads to another provider. The service levels agreed therein never foresee a 100% service continuity, as parties understand and agree that the service will not be the same during a termination phase as during the operational phase of the contract. Parties also know that business and service continuity is better guaranteed through collaboration between the service providers (both the incumbent and new service provider) and the client, rather than through shifting obligations onto the incumbent provider.

In light of the above, we suggest following amendment to this provision:

> *New Article 23(3)* ***Without prejudice to the originating providers' obligations, all parties involved, including destination service providers, shall, where applicable, collaborate in good faith to make the switching process effective.***
>
> *24.1(a)(2). ensure* ***~~full~~ compliance with the contractual arrangements related to*** *continuity in the provision of the respective functions or services.*

Article 24.1(a) is again based on the assumption that the incumbent provider should be responsible for the whole switching process, whereas switching should be a joint responsibility between both providers and the customer to be a workable, stable and smooth process. Therefore, Article 24.1(a) should be amended as follows:

> *Art. 24.1(a)* ***reasonably*** *assist,* ***~~and~~*** *where technically feasible,* ***~~complete~~*** *the switching process;*

4 - Scope of the porting obligations - Article 24.1(b) contains a sweeping, all-encompassing obligation to port "at minimum" all (i) data imported by the customer at contract start; and (ii) all data and (iii) metadata created by the customer and by the use of the service. While there is no doubt that data imported or created by the customer should be exportable, the need to port all metadata is questionable. The broad scope of Article 24.1(b) may result in overloading the switching process, and therefore jeopardise the success of these sometimes-complex projects.

Therefore, in view of keeping a reasonable balance between a successful migration and the right for customers to obtain metadata should this be necessary (which we believe is the Commission's intent), we would suggest the following amendment to Article 24.1(b):

> "*(b) an exhaustive specification of all data and application categories exportable during the switching process including, at minimum,* ***and only to the extent technically feasible (e.g. when a cloud user has selected portable data formats)***
>
> i. *all data imported by the customer at the inception of the service agreement and,*
> ii. ***to the extent these data and metadata are necessary for the customer to receive the services from the new provider of data processing service****, all data and metadata created by the*

customer and by the use of the service during the period the service was provided, including, but not limited to, configuration parameters, security settings, access rights and access logs to the service,

being understood that providers of data processing services shall not be required to disclose trade secrets or other proprietary information".

5 - Functional equivalence Articles 26.1 and 2.16 set an obligation of result for the incumbent IaaS provider to ensure **the same service parameters** in the environment of one of its competitors. **This is confusing, legally, operationally and technically.** It is indeed hard to understand what is precisely expected from the incumbent provider. In other words, *how* is it envisaged that a provider will ensure the same level of security and performance, and even more so the same quality of service, output and performance in the environment of one of its competitors?

Should the incumbent provider have access to its competitors' environment? If so, how can the new provider ensure security of its environment? Or should the incumbent provider compare service level agreements? Should it audit the environment of the new CSP? Or is it just jointly liable for an area over which it has no control? And what happens if the customer does not contract the same level of service because it deems it doesn't need the same level of service?

Also, functional equivalence as envisaged could eliminate competitive advantages that IaaS providers use to differentiate, because:

- it forces CSPs to share intellectual property, trade secrets, and other competitive advantage with competitors, to ensure they are able to provide the same function/capabilities; and

- it incentivizes clients to select the cheapest service available given their former provider is responsible to ensure they benefit from the same service parameters (such as security, features, availability, etc.), **thereby** blocking innovation, optimization and differentiation.

We believe that to achieve interoperability in the IaaS sector, (i) the scope of any potential functional equivalence requirements should be agreed with the customer in the contract; (ii) interoperability and any functional equivalence related thereto should be a joint task for both the incumbent and the new provider; and (iii) providers should not be performing work outside their environment.

The following amendments are suggested:

Article 2(14) 'functional equivalence' means ***a definition as agreed upon by a customer and provider of data processing services, or*** *the maintenance of a minimum level of* ***pre-defined*** *functionality* ~~***in the environment of a new data processing service after***~~ ***during*** *the switching process, to such an extent that, in response to an input action by the user on core elements of the service, the* ~~***destination***~~ *service will deliver the same output at the same performance and with the same level of security, operational resilience and quality of service as* ***agreed in*** ~~***the originating service at the time of termination of***~~ *the contract.*

Article 26.1 ***The incumbent and the new*** *provider*~~***s***~~ *of data processing services that concern scalable and elastic computing resources limited to infrastructural elements such as servers, networks and the virtual resources necessary for operating the infrastructure, but that do not provide access to the operating services, software and applications that are stored, otherwise processed, or deployed on those infrastructural elements, shall* ***provide reasonable assistance 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***~~ ***with a view on achieving*** *functional equivalence* ~~***in the use of the new service***~~*.*

Article 26.3 For ***all*** *data processing services* ~~***other than those covered by paragraph 1***~~*, providers of data processing services shall ensure compatibility as agreed upon by the parties with open interoperability specifications or European standards for interoperability that are identified in accordance with Article 29(5) of this Regulation.*

6- Open interfaces Article 26(2) sets an obligation for providers of data processing services that are not IaaS to adopt open interface publicly available and free of charge. However, the current wording of the text could lead to diverse interpretations of what constitutes "open interfaces" and lead to the adoption of interfaces with extremely different degrees of openness and therefore would not reach the announced target of solving the lock in, problem cloud customers are facing on the European market.

Therefore, a definition of "open interface" is also needed to better understand how those obligations will be applied. Currently a few cloud services are already characterized by full competition (i.e., no lock in, no lock out and fair contractual practices). Therefore, clarifying the meaning of open interfaces could also provide clarity on the regulatory treatment of those specific service types.

In addition, open interface being publicly available is a key element to ensure fair competition between cloud providers and avoid that gatekeepers could lock our European small software providers to access cloud infrastructure and develops new services and sell innovative cloud solution on the European market.

The following amendments are suggested:

(New)Article2(23) Definition of open interface

Article 2(23) '***open interface' means a publicly available, standardised, and programmable mechanism to access capabilities in a cloud service or software from other services or software. Such interface implies that more than one program exists to interface with the application that has an open interface or that a program can be readily written to communicate with it. Furthermore, open interface implies that all key services and features are available to be accessed via these interfaces, rather than being held privately only for the service provider to access.***

6 - The financial restrictions of Art. 25 also raise questions: if additional obligations and responsibilities are imposed on a Cloud provider when a client terminates a cloud contract, should these be provided at cost for 3 years and then for free (resulting in the provider making a loss)? This would be especially unreasonable if the contract is terminated due to the customer's breach.

We believe the objective should be that customers be made aware of what it would cost them to enter into a specific contract. Customers are able to review the relevant information to calculate the total cost of ownership (TCO) of selecting a specific vendor over another. Therefore, it would be fairer to all if the costs were transparent and communicated well in advance rather than asking providers to not invoice the switching services they provide.

From [date X+3yrs] onwards, providers of data processing services shall not impose charges on the customer for the switching process, ***unless a clear basis for the calculation of these charges has been communicated before the start of the contract****.*

Chapter VII – International transfers and government access

Regulation should strive to solve conflict of laws, not reinforce them, and we believe conflict of laws should be solved through multilateral government talks, not by one government regime imposing unilateral requirements on a specific sector.

Personal data and non-personal data are different in nature, requirements and legal mechanisms and these differences should be accounted for in policies addressing international transfer of data and government access to data.

GDPR clearly sets forth 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.

Cloud users, unlike cloud providers, know their data. Practically this means users know whether their data is subject to trade secrets, IPRs, national security schemes or other Union or Member State law. Cloud providers typically do not have access to data stored or hosted on behalf of their clients and are not able to determine what legal restrictions may apply to the data that they are processing. Similarly, they do not have sufficient visibility of the laws and surveillance practices employed by sovereignty governments outside the EU that could result in unlawful data access. Therefore, in practice, these providers will have no way to comply with Article 27.1.

> *Art. 27.1* ~~***Providers***~~ ***A customer*** *of data processing services shall* ***instruct the provider of data processing services to*** *take all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where* ***customer has determined and informed the provider that*** *such transfer or access would create a conflict with Union law or the national law of the relevant Member State, without prejudice to paragraph 2 or 3.*

The "data holder" is a defined term under Article 2(6) of the Data Act and refers to the entity that must share data under Chapters II and III of the Act. Therefore, it seems that this term should not be used in Article 27, as this would cause confusion. We suggest editing Art. 27.5 as follows:

> *Art. 27.5 The provider of data processing services shall inform* ***its customer*** ~~***the data holder***~~ *about the existence of a request of an administrative authority in a third country to access its data before complying with its request, except in cases where the request serves law enforcement purposes and for as long as this is necessary to preserve the effectiveness of the law enforcement activity.*

Chapter VIII – Interoperability

Article 28 sets forth essential requirements regarding interoperability for operators of data spaces. It is therefore of paramount importance to define which entities are "operators of data spaces". Platforms that serve to exchange data should not be subject to these requirements by default. For example, some platforms used today work very well to exchange data, and these platforms are not Blockchain enabled as required by Article 28.1(d).

These requirements however all make sense for the well-defined upcoming Common European data spaces. We therefore suggest following amendments to Article 28.1:

> *"Operators of **European Common** data spaces shall comply with the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services."*

While we agree that the European Commission should be able to adopt common specifications regarding essential requirements for smart contracts as set forth in Articles 29.5 and 30.6, we believe that the industry should have the opportunity to finalise standardisation activities, and that the Commission should intervene only when a standardization request results in an insufficient standard that does not address the concerns expressed in Articles 29.1 and 2, or 30.1(a) to(d), respectively.

> *Where harmonised standards referred to in paragraph 4 of this Article do not exist, **the Commission shall issue a standardisation request in accordance with Article 10 of Regulation 1025/2012. ~~or w~~ Where** the Commission considers that the **~~resulting~~ relevant** harmonised standards are insufficient to ensure conformity with the essential requirements in paragraph 1 of this Article in a cross-border context, the Commission may, by way of implementing acts, adopt common specifications in respect of the essential requirements set out in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2).*

Article 30 sets forth essential requirements regarding smart contracts for data sharing. The essential requirements of Article 30.1(b) and (c), as they relate to termination and interruption of smart contracts, data archiving and continuity, would best be applied to smart contracts that allow the exchange of value or assets such as cryptocurrencies. The rationale is that the requirements on termination and interruption of smart contracts set forth in Art. 30.1(b) aim to address issues and disputes that could financially harm a Blockchain participant.

Also, archiving data for continuity purposes as required under Art. 30.1(c) will serve auditability and dispute resolution objectives, which again are useful in the framework of exchanging values or assets and are not required for other types of smart contracts, such as those deployed in member only Blockchain enabled platforms.

There is no doubt that access control mechanisms as referred to in Article 30.1(d) should be implemented. However, their level of implementation will depend on the type of smart contract, and hence on the access controls necessary for that specific smart contract (i.e., the specific Blockchain application). For example, in the case of a permissioned Blockchain that only the members of the application are entitled to enter, access control is inherently imposed. But if the purpose and use of the Blockchain application is to share information with a wide audience, access controls may not be required. Therefore, the requirement that "access control must be protected at the smart contract layer" is problematic and should be removed.

To address all the comments made above, we suggest amending Art. 30, by removing the limitation to the smart contract layer at the end of Article 30.1.d, and add a necessary clarification in relation to Article 30.1(b) and (c), as follows:

1. *The vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of an agreement to make data available shall comply with the following essential requirements: […]*

(d) and access control: a smart contract shall be protected through rigorous access control mechanism ~~***at the governance and smart contract layers***~~*.*

Sub-paragraphs b) and c) shall only apply to smart contracts that allow the exchange of value of assets.

Chapter IX - Implementation and Enforcement

In the Commission proposal, enforcement is done by Data Protection Authorities, and authorities to be set up by Member States (incl. to enforce the cloud switching requirements of Chapter VI). At the same time, it is stated that "the authority of sectoral authorities shall be respected", but it is not clear whether this mean they should be involved, consulted or competent.

We caution against this framework, which will undoubtfully lead to fragmentation and call for competence of a pan-European enforcement body, responsible to provide official interpretation of the regulation, while the national supervisory authorities' guidance should not be binding. Also, we urge lawmakers to think of other ways to further avoid fragmentation, such as a one-stop-shop mechanism with one lead authority, or the implementation of a specific unit within the national Data Protection Authorities, responsible for issues related to, non-personal data sharing. This could be more efficient than assigning competence to separate bodies, because in any event, DPAs will be competent for matters related to mixed data sets.

About AIOTI

AIOTI is the multi-stakeholder platform for stimulating IoT and Edge Computing Innovation in Europe, bringing together small and large companies, 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.