ITI Promoting Innovation Worldwide

03/09/2021

# ITI's Response to Data Act Public Consultation

## Introduction

The Information Technology Industry Council (ITI) is the premier global advocate for technology, representing the world's most innovative companies from technology, hardware, software, services, and related industries. Our industry shares the Commission's goal to further and facilitate data access and use. Preserving an enabling environment for data-driven innovation, including through the Data Act, is essential to pursue this goal and ensure the global competitiveness of Europe's digital economy.

We appreciate the opportunity to provide our feedback on the Data Act public consultation in the following pages, with the goal of ensuring that the future Data Act becomes an innovation-enabling tool for the EU's data economy.

Generally, in moving towards the Data Act proposal, the best approach to improve access to data in business-to-business (B2B) or business-to-government (B2G) scenarios is to focus on incentives for companies to engage in data sharing. This will better take into account the protection of trade secrets and intellectual property (IP), and also avoid disincentivising companies' investments in data innovation. On the other hand, we strongly recommend avoing any approaches based on mandatory requirements, which would have adverse effects on companies which would no longer be incentivised to innovate and develop new services. In addition, the Data Act should encourage and support the flow of non-personal data across borders. Any measure potentially restricting international data flows should be avoided as much as possible, to enable businesses in the EU to grow and compete internationally.

## 1. Business-to-government data sharing for the public interest

While we share the fundamental goal to promote fair and transparent B2G data sharing, our industry is concerned about options to introduce with the Data Act mandatory sharing schemes or right to access privately held data from the public sector. These provisions would constitute a significant departure from current practices, and may give rise to privacy, security and competition concerns as well as risk chilling public-private cooperation and service provision. Private sector data is very often the product of investment and innovation, and it can be sensitive or give insights into sensitive business or technical information. Thus, B2G data sharing should be incentivised in a flexible framework and by encouraging investments in privacy-enhancing technologies but remain voluntary in all cases.

Having said that, the Data Act framework is well placed to harmonise existing legal frameworks on B2G data sharing at Member States level, which are sometimes inconsistent with rules on IP, privacy and competition all covering certain angles. A harmonized framework at EU-level would benefit legal certainty and incentivise voluntary B2G data sharing agreements.

*Global Headquarters*
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

*Europe Office*
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

In order to pursue specific public interest goals, data access requests by public bodies should be proportionate and motivated, balanced and limited to the minimum extent necessary for the performance of a specific function. The definition of "public interest" data should also follow a context-specific approach, be assessed on a case-by-case basis and be defined as narrowly as possible. An unclear definition of public interest may lead to problematic scenarios whereby businesses share data with the public sector without any guarantees of how the data will be used. A continuous discourse between policymakers and stakeholders to shape the criteria in a proportionate manner should be preferred.

The Commission should identify critical application fields for B2G data sharing such as healthcare and emergency response, and at the same time specify what types of data sets it finds valuable and why. Public sector bodies should also be transparent regarding the types of safeguards applied to the protection of commercially sensitive data, IP, trade secrets and privacy. This would enable and incentivise companies to discuss and forge voluntary data sharing agreements with public entities. These agreements should allow companies to provide data to the public sector at different rates depending on the purpose of the data use.

## 2. Business-to-Business data sharing

Our industry supports the goal of increasing data sharing and improving access to data for SMEs and start-ups. Incentives rather than mandates are the most effective tool to encourage data sharing for companies while safeguarding companies' investments in data innovation, as well as trade secrets and IP. We welcome references in the questionnaire to safeguarding freedom of contracts in B2B data sharing. In order to promote legal certainty, it is also important, as mentioned in the questionnaire, that the Data Act is coherent and does not overlap with existing legislation in the field of data protection and competition.

Companies have to make several considerations before engaging in voluntary data-sharing, involving a consideration of risks to which the data may be exposed and of existing contractual obligations. In particular:

- entities are subject to a wide array of legal obligations depending on the data use, and the jurisdictions where the data is stored and processed.
- Second, entities need to consider all contractual obligations as well as the impact of upstream and downstream agreements on the data collection, use and disclosure.
- Third, different sectors have completely different needs to share or acquire data with or from other businesses. Even businesses within the same sector might have completely different data strategies.

*"Our industry supports the goal of increasing data sharing and improving access to data for SMEs and start-ups. Incentives rather than mandates are the most effective tool to encourage data sharing for companies while safeguarding companies' investments in data innovation".*

Due to these considerations, voluntary agreements between companies constitute today the main tool for B2B data sharing, and several consultations at the EU level in the past few years

confirmed that there is no demand to create legal obligations in this area. Therefore, ITI believes that maintaining the current flexibility of voluntary agreements in the Data Act is the appropriate way forward.

The proposal to introduce model contract terms recommended by the Commission as sketched out in the questionnaire of the consultation could represent an innovative tool to promote trust in B2B data sharing arrangements and increase access to data sharing for SMEs – insofar as, as the questionnaire recognises, any such mechanism remains voluntary and does not prejudice the possibility for companies to dispose of their data and freely conclude contractual arrangements for data sharing. The Commission should promote the use of existing Open Data Agreements such as the Community Data License Agreements, or specify who will draft the model contractual terms and ensure that the terms are developed through a continuous and regular dialogue with industry stakeholders and developed in line with industry and sector specific best practices, to ensure that the model terms are practical, easily applicable and future-proof.

The proposal to introduce a "B2B fairness test for all B2B data sharing contracts" seems vague: it is unclear whether it would be optional or mandatory, who would oversee carrying out such tests and how it would impact existing contractual arrangements. In addition, the questionnaire mentions that the fairness test "would only address excessive clauses" while leaving all other terms to contractual freedom. It is not clear what is meant here by "excessive clauses", which criteria will be used to define them and how would these criteria be justified. In addition, it is unclear how notions like "stronger negotiating power" would be defined. The Commission should consider the impact of any such measure, and avoid introducing uncertainty into business models, or risk slowing down contracting between commercial actors. Industry stakeholders should be consulted on the substance of the test and involved in its potential definition. We also question the applicability of FRAND principles to data licensing, since it is unclear how this would work in practice and what the principle of "transparency" would entail. Much more work needs to be done to analyse and explain all possible consequences of applying FRAND outside of the context of patents and standard setting organisations. The Commission should consider that an excessive compliance burden on companies that wish to enter data sharing arrangements may become a disincentive to share data, and therefore run counter to the very objective of the proposal.

Finally, the questionnaire floats the proposal to introduce horizontal access modalities to regulate how sectoral data access rights established by other pieces of legislation are exercised. While further details on how this would work in practice are yet to be seen, the applicability of horizontal access modalities to different sectors, with different data sharing practices and data strategies is questionable. While sharing obligation may be acceptable in some narrow and specific cases, any type of B2B data sharing obligation should remain limited to existing sharing obligation and aligned with

> ***"Companies should remain in control of their data, as any mandatory sharing scheme would risk disincentivising investment in data innovation as well as putting at risk IP, trade secrets and privacy".***

existing competition rules. Companies should remain in control of their data, as any mandatory sharing scheme would risk disincentivising investment in data innovation as well as putting at risk IP, trade secrets and privacy.

## 3. Tools for data sharing: smart contracts

Smart contracts are an ideal tool to record real-time data generated by IoT devices onto a secured ledger, and thereby capture immutable records and provide trusted transactions. Also, the benefits of blockchain technology can be leveraged to support the goals of GDPR, and smart "contracts" can be a very effective tool to implement data sharing, provided harmonisation of regulatory requirements is ensured and technical considerations, such as interoperability, are addressed through global industry-led standards.

In considering the possibility to lay out a mandate for European Standardisation Organisations to establish harmonised standards for smart contracts interoperability, the Commission should ensure that standards do not become a market entry barrier. In order to avoid potential fragmentation in global markets, the EU should rely on global, voluntary industry-driven standards to ensure the availability of state-of-the art technology and technical solutions. The Commission should also assess how potential requirements set by the Data Act would impact innovation in the field.

## 4. Clarifying rights on non-personal Internet-of-Things data stemming from professional use

Any measures aimed at regulating access to and use of machine-generated non-personal data should be proportionate and take into account the potential risks that may arise from disclosure of certain data, especially regarding the exposure of IP, commercially sensitive information and trade secrets as well as potential risks to privacy.

In looking at the IoT ecosystems and potential challenges related to access and use rights of IoT-generated data, we encourage the Commission to avoid solutions that would entail mandatory data-sharing schemes, as these may discourage investment in data innovation and risk exposure of sensitive data. In addition, considerations around "market fairness" challenges posed by IoT data should be based on existing competition law concepts and avoid overlaps with existing legislation in the field.

## 5. Improving portability for business users of cloud services

Our industry supports increasing cloud portability and we have been committed to the work of the SWIPO process and contributing to the adoption and implementation of the Codes of Conducts on cloud switching and data portability. Considering that the Codes have been active for one year, the programmed evaluation of the Codes of Conducts should prompt a discussion between the Commission and industry stakeholders, in SWIPO and more broadly, to assess the most appropriate way forward to pursue the shared goal of increasing cloud portability. The introduction of the Cloud Rulebook can as well give more visibility to the SWIPO initiative, and therefore increase its impact. For these reasons, proposals to include binding obligations for cloud portability in the Data Act are premature at this stage.

In general, options to introduce legal requirements based on SWIPO are premature, and we caution against taking such approach at this stage. Should the evaluation of SWIPO show no impact, any action on data portability must be targeted, take specific situations and contexts into account and avoid a one-size-fits-all approach. Proposals on switching, access to data and portability should consider the data at play, the operator concerned and available alternatives. Porting requirements should be solely targeted at making the necessary tools available to cloud services' customers, in order for them to port their data, and fees for egress should remain fair and transparent. It is important to stress that portability and switching are complex and cannot be limited to data portability issues. It is therefore key to distinguish simple migration of stored data – GDPR-type of portability requirements - from migration of an entire environment/application. The latter requires to move a significant amount of data with specialist technical assistance and careful project management. This also requires defining measures to mitigate business interruption. The cost related to this operation is unavoidable. Having switching costs does not mean that a company is locked-in, but the cost will just depend on the complexity of the switching operation. Mitigating potential switching costs requires good architecture, standard deployment practices, and pre-planning.

*"Should the evaluation of SWIPO show no impact, any action on data portability must be targeted, take specific situations and contexts into account and avoid a one-size-fits-all approach."*

In addition, the imposition of rigid standards to enable data portability could have unintended consequences, like hardwiring the status quo, forestalling innovation by homogenizing offerings that would reduce competitiveness, customer choice and precluding future portability. Cloud computing cannot be reduced to simple hosting and includes many more complex services - from computing to AI - that cannot be standardised unless at the cost of innovation. A customer makes the choice of a particular CSP not because of the vendor but because the technological approach allowing for speed and agility to meet their specific business needs. This is particularly true for data-intensive AI applications, which, due to their diversity, require the recognition of the importance of sector/application-specific approaches; one approach will not fit all AI applications.

## 6. Complementing the portability right under Article 20 GDPR

The technology industry has made major efforts to comply with new rules brought about by the GDPR that have entered into force only a few years ago. Mandating additional rules at this stage with the Data Act seems premature and would impose burdens on companies that should not be underestimated, while affecting innovation in Europe.

The questionnaire suggests enhancing the portability right for individuals under Article 20 of the GDPR by establishing technical specifications to mandate technical interfaces that enable real-time portability. We strongly urge against this approach: while Article 20 of GDPR aims to facilitate the switch for users from one service provider to another, it does not require

continuous data flows. Thus, real time portability is neither necessary nor a condition for moving personal data from one service to another. Real time portability will also ignore that the user will still need to consider locations of back-up, the format of its choice, the required IT configuration of the destination system as well as the necessary network bandwidth for the transfer. In addition, real-time processing of access or portability requests may also give rise to privacy concerns. It is thus unclear how a data controller under GDPR shall ensure real time flow of data while complying with conflicting rights of third parties or statutory obligations. Finally, it is important to consider that Article 20 of the GDPR only applies to cases such as consent, contract performance or automated processing.

Consumer choice and consumer-friendly product innovation will lead to more interoperability between products and services. For this reason, while implementing data portability is a priority for our industry, mandating technical specifications would not be the correct approach. Instead of imposing technical specifications, the Commission should look at an approach based on providing transparent information to users. In a B2B context, this could mean providing detailed, clear, and transparent information regarding the processes, technical requirements, timeframes, and charges that will be applied should users want to switch to another provider or port data back to their own IT systems.

It is also important that the Commission relies on global, industry-driven standards agreed upon in international standard development bodies for the most appropriate technical solutions to comply with regulatory requirements. Mandating technical specifications in this context would risk fragmentation in global markets and potentially create regulatory divergences globally. The European Commission should also provide clear guidance on legal compliance, especially with the GDPR. Without standardised best practices, organisations may be reluctant to assume liability risks of using data from third parties. Such issues can be addressed by endorsing industry standards and model data governance frameworks.

Before considering legal requirements, the Commission should thus take into account ongoing industry initiatives such as the Data Transfer Project (DTP) which promotes direct portability among service providers. Companies are making progresses to improve their own portability offerings by adding new features (like the option to select specific subsets of data) and to invest in the success of the Data Transfer Project by supporting partner onboarding and incorporating the DTP protocols on their own service. Such initiatives could be supported, expanded and replicated in the 'smart home' area.

## 7. Intellectual Property Rights – Protection of Databases

The review of the 1996 Database Directive for the purpose of assessing the role of machine-generated data should be carefully assessed. While we welcome the Commission's goal to provide more legal clarity, proportionality, consideration of companies' data-related investments and a high level of protection of business secrets should remain at the basis of the Commission's assessment.

The Commission should consider that the CJEU has extensively confirmed that created data falls outside the sui generis right. In addition, any plans for a specific access regime to facilitate

trading in and access to databases should consider potential overlaps with other intellectual property rights. For example, copyright regulates access to protected subject-matter throughout several EU instruments, such as the new text and data mining exception in Directive 2019/790, which applies to both copyright and the sui generis right on databases. A mapping and evaluation of existing laws and regulations both at EU and national level is advisable before proceeding with a review of the Database Directive. An access regime might also conflict with data protection legislation, such as the GDPR and it could conflict with existing contractual obligations that contractual parties cannot unilaterally waive due to a future obligation (such as limitation of usage rights of data or confidentiality obligations).

Finally, as regards the protection of trade secrets, it is important that any clarification of the application of the Trade Secrets Directive does not limit protectable data to data which meets the legal definition of a trade secret. Data should be capable of protection by contract, since it may itself constitute confidential or sensitive information, or may give insights into confidential or sensitive technology.

## 8. Safeguards for non-personal data in international contexts

***"Organisations should be able to leverage the best available technologies and service providers, regardless of their location, to remain competitive. The important enabling function of global data flows should accompany the consideration of any policy initiative."***

The free flow of data across borders should be encouraged and supported with the Data Act, and the Commission should be cautious about introducing any new measure potentially restricting international data flows. The ability to transfer and access data around the world is critical to all economic sectors and companies of all sizes, and especially allows smaller players like SMEs and start-ups to benefit from innovative solutions, minimise costs and reach consumers globally. Organisations should be able to leverage the best available technologies and service providers, regardless of their location, to remain competitive. The important enabling function of global data flows should accompany the consideration of any policy initiative. Before introducing new measures, the Commission should first seek to alleviate any concerns about foreign governments access to data through multilateral discussions among like-minded governments instead of imposing regulatory requirements on the Cloud sector, and also consider long-standing international agreements and treaties regarding IP (e.g., the TRIPS Agreement or the Berne Convention) which are currently enforced and provide protection for data protected by IP and trade secrets. Data localisation is not a solution to perceived risk around exposure to foreign jurisdictions. It should be stressed that the location of the data does not have an impact on whether foreign laws apply to a provider. Rather, it is paramount to avoid conflicts of law and encourage multilateral cooperation among like-minded partners, for instance at OECD level.

In general, it is not clear how the question of third-country access to non-personal data ties with the Data Act. There is a need for clearer procedures and guidelines for sharing data with law enforcement or government authorities within the EU and externally with third countries.

However, any work in that realm should aim at avoiding legal frictions and build on existing workstreams, such as on the e-evidence proposal, the OECD work on law enforcement access to data held by private companies, the Budapest Convention and ongoing international negotiations. An additional piece of legislation like the Data Act would not increase legal certainty and potentially create more conflicts of law.

The option to create an obligation to report all law enforcement access requests to users, as mentioned in the questionnaire, would not always be possible in practice, even within the EU. There may even be exceptional cases in which requiring notice to a user may be counterproductive and could lead to harm to another person or to the destruction of evidence. Moreover, customers are generally the controllers of the data in question and cloud service providers are not always in control of who the customer has provisioned accounts to (e.g., employees, students etc) or on where the users are located.

The second proposed measure to report all the foreign laws with extraterritorial effect to which a cloud provider is subject should be relevant, proportionate and tailored to the risk. As a principle, any transparency measures in the Data Act should be applicable to all Cloud Services Providers active in the EU Single Market and must ensure a level-playing field, be proportionate to the risks and non-discriminatory. This should also take into account that it is not useful for cloud customers, users or the general public to obtain a long list of laws with extraterritorial effect to which all entities of a multinational group are subject to (e.g., Tax laws, non-Bribery regulations). Therefore, the scope of the obligations should be carefully crafted to avoid any unnecessary burden that would only result in confusion. In addition, due to the complexity of data flows in a global economy, the dynamism of regulation across the globe, cloud providers may not be able to provide advance notice of this information. In some cases, since cloud service providers and customers operate on the basis of shared responsibilities, the customer may be in charge of assessing compliance with the laws it is subject to. The Commission should also consider that smaller players such as start-ups may lack capacity to comply with such reporting obligations. To avoid creating a burden for companies and negatively impacting innovation, flexibility of requirements and proportionality should be the overarching principles in further considering this aspect.

The option to extend to cloud providers the requirements on international access of the Data Governance Act proposal seems potentially very challenging in practice. More clarity would be needed on what type of “legal, technical and organisational measures” cloud providers should put in place to prevent access to data from third-country governments. It is unclear who would assess such legal, technical or organisational measures - an important detail, considering the profound consequences such an assessment would have on the market. It also seems probable that such measures would create conflicts of law rather than resolving them. Finally, as the Data Governance Act is yet to be approved by the co-legislators, the possibility of extending its regime on third-country access to non-personal data to cloud service providers appears like a potential source of legal uncertainty and should be carefully considered in the development of the Data Act.

Given that non-personal data is less likely to be subject to access requests, for instance for law enforcement purposes, it would be useful to better understand which specific situations

the Commission envisions when talking about such requests. In general, it is important to consider that non-personal data do not pose the same risks as personal data, for instance in terms of fundamental rights, and as such, any policy measure in this regard should be proportionate to that lower level of risk.

We would welcome further discussions with the European Commission on issues related to international access and cross-border data flows. ITI calls for constructive multi-stakeholder dialogues with all Cloud Services Providers and other relevant actors, regardless of their place of establishment, and cloud user groups, to shape sound and proportionate obligations related to technical, legal and organisational measures.

***