ITI Promoting Innovation Worldwide

13 May 2022

ITI Comments to the Data Act Proposal

1. 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 membership is active across the entire spectrum of the data value chain, and it includes data processing service providers, IoT manufacturers and users and many other types of data-driven innovators who have been shaping and supporting the data economy in Europe and globally.

We appreciate the opportunity to provide feedback on the Data Act proposal. We support the goal of the proposal to facilitate data access and use, and promote data sharing while preserving incentives to invest in data innovation and in the EU Digital Single Market and safeguarding individuals' rights.

These objectives could be best achieved through ensuring legal, political, and policy alignment with existing EU data regulation, **and encouraging sharing of data between companies on the basis of contractual agreements that can effectively protect businesses' investments in data innovation** and provide safeguards against unfair competition and disclosure of IP and trade secrets. Our industry is also supportive of efforts to improve switching between cloud service providers (as defined within the Proposal as "data processing services") and data portability in a way that is technically realistic, meaningful for the user and economically viable.

The Data Act should avoid imposing rigid standards for portability, while taking specific situations and contexts into account and considering the data at play, their volume, the operator concerned, and available alternatives. It should also take into account existing contractual arrangements between cloud providers and cloud customers, as well as the specific legal and financial obligations of those cloud providers that are publicly traded companies. Specifically, we have concerns regarding the appropriateness of the proposed contract minimums for B2B data processing services, as such contracts are negotiated between sophisticated parties and often operate on multi-year terms. **We also strongly urge lawmakers to avoid any disproportionate restriction to international data flows** which would risk adding further complexity to international data transfers, given the Data Act's focus on non-personal data.

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

The sections below contain more specific comments and recommendations for policymakers on the different sections of the proposal.

2. Access and use rights for users and third parties – Chapters 1,2 and 3

ITI supports the broader goal of the Data Act to increase data sharing, access and use as a catalyst for growth, innovation and for the delivery of new and better services to consumers. Currently, voluntary agreements between companies constitute the main tool for business-to-business data sharing, and many obstacles may arise when a company decides to share its data. These include the assessment of different legal obligations, both upstream and downstream contractual agreements and diversity of data strategies across sectors or even within the same sector. Trust is also a fundamental element of this assessment, as businesses want to make sure that privacy and data are protected, that they will not be exposed to liability for negligent or malicious use, and their investments in data innovation are not undermined by trade secrets or intellectual property disclosures. To increase data sharing, we agree that it is important to address these obstacles and incentivise companies to share more data.

Chapters 1, 2 and 3 of the Data Act go beyond incentives and mandate access and use of all data (personal and non-personal) generated by connected products for users, and user-designated third parties. The scope of this mandated access is unclear, as the proposal addresses data at a broader scale at various places. This approach will drastically change the way companies govern data and impact a variety of fields, including data protection, competition, trade secrets and IP protection and product design. ITI has a number of recommendations to address these issues, as outlined further below. It is fundamental that the Data Act framework supports the goal to increase data access and use in a way that is meaningful for the user and without undermining businesses' investments in data innovation and market incentives to share data. In order to do so, we urge policymakers to focus on the points below:

Clarify key concepts

Lawmakers in the Parliament and the Council should seek to clarify some key concepts and definitions at the core of Chapters 1, 2 and 3.

Article 2(1) of the Data Act makes a **broad definition of data**, which includes all data generated by the use of a product. **It is however unclear from the text of the regulation whether technical critical data that are relevant to the integrity of the product would also be included in the scope.** We would oppose such inclusion, given that technical critical data would give insight on sensitive information that is paramount to upholding the integrity of the product and therefore should not be subject to broad data access requirements. These data would include passwords, encryption information, unique IDs of the user used for tracking, software variant information, application usage data, diagnostic data, and

application performance data that may be derived from user experiences but are used for product improvement. Amending the definition of data in this manner would then more efficiently align with the EC's objective of enabling greater third-party data access while increasing trust. It would enable data access that is actually useful for third parties to offer novel business services, rather than threaten the integrity of manufacturers investments into the very devices that enable such data generation and subsequent third-party access.

In addition, **each chapter also applies to different types of data** with some provisions scoped only to non-personal data (e.g., the restrictions on data transfers). Yet, particularly in a consumer IoT context, it is unclear which 'generated data' would not be personal data already falling under GDPR rules. At the same time, the scope of Chapter 3 is broader than Chapter 2 and includes scenarios where a "data holder is obliged to make data available to a data recipient under other Union law or national legislation" (art. 8(1)). To increase clarity of the regulatory framework, we suggest ensuring that the scope of this Regulation cover that only data strictly generated from an IoT/connected product or related services. In addition, the proposal should not require business to collect and retain more personal data. For example, it requires companies to make "by-products" like data created in stand-by mode (recital 17) available to share with third parties. However, for some products like virtual assistants, such data are usually not retained permanently (in fact, they are usually just kept temporarily on the device memory and overwritten every few seconds). Sharing requirements of such data would result in retention of more, often sensitive data, thereby standing in contrast with data minimisation principles of the GDPR.

Greater clarity in the **definitions of "data holder" and "data user"** would be necessary to avoid any confusion regarding who is owning and controlling the data. In the context of cloud services, for example, customers are provided assurances, both contractually and technically, that they own and control their data. Many IoT products are often powered by cloud services, which act as data processors under the GDPR and process mixed datasets. In this context, it is not clear whether a software developer that sells the software to its customers who then implement it in an IoT device should also be considered a data holder. This should not be the case because a general-purpose software developer is not entitled to access the data generated by the usage of an IoT device. Moreover, it is **unclear what role is expected of such companies that would be considered data processors under the GDPR.** While for personal data Recital 24 equates the data holder to a data controller, the definition of data holder in Article 2(6) considers that for non-personal data any entity that has the technical ability to make the data available should be considered the data holder: this double standard is not justified, the same type of criteria should apply to personal and non-personal data. This becomes more complex in B2B environments and contractual arrangements where many different platforms and services are implicated in complex ecosystems of "products" and "related services". It would thus be helpful, and important, to establish a **clearer definition of data holder for non-personal data and use the well-known definitions of data processor and data controller also in the context of the Data Act. This could easily be clarified by**

ensuring that parties can agree compliance obligations through contractual arrangements. In this regard, only business customers, i.e., companies that own and control the data, should be defined as "data holders" and face the related obligations of the Data Act.

The definition of product should also be further clarified. While it seems clear that the objective of the regulation is to cover broadly 'the Internet of Things (IoT)' (recital 14), while excluding devices that are "primarily designed to display or play content or to record and transmit [it]," (recital 15) such as smartphones or tablets, it is unclear how the regulation would apply to cases where for instance such devices are used to control the IoT product. In addition, other products not mentioned in recital 15 but which are also used primarily to display content, such as printers, should be added in Recital 15 for clarity and completeness. Policymakers should also seek to clarify how Chapter 2 would apply to products that are used by multiple users and where it is not possible to trace the data back to one single user. To increase clarity, we also suggest referencing Recital 15 in the body of the Regulation.

Policymakers should also **clarify the requirement in article 3** for which products shall be designed and manufacturers to allow that data are accessible "**by default, easily, securely and, where relevant and appropriate, directly."** It is important to take into account that from a technical perspective it is not feasible to realise the constant availability of all generated data from certain products, both because of the amount of data for certain industries (e.g., automotive) or in case the data themselves are not available to the manufacturer (e.g., OEM). The implementation of these requirements would require massive investment in data governance and/or process delivery and data architecture and create significant costs for companies in the EU, and this should be reflected in the implementation timeline.

Another important clarification that lawmakers should explore is the **difference between scenarios in which the user is a consumer (b2c) and those where the user is a business (b2b).** In the b2b context, it is unclear how the regulation would work in complex IoT environments, where several actors provide "related services", which according to recital 16 would be in scope of the data access rights, and have different roles with regard to the data generated by the product. In complex IoT environments, IoT data is communicated and transformed through various captors, sensors and robots, which could also generate IoT data, thus multiplying the number of data holders and data users in ways that are both complex and evolutive in time.

The b2b/b2c differentiation seems needed for instance in the context of the requirements in article 3(2) to provide information to users before "concluding a contract for the purchase, rent or lease of a product or a related service," on a variety of things, including the nature and volume of the data generated (art 3(2a)) or whether and for what purpose manufacturers intend to use the data generated by the product (art. 3(2d)). This may be less relevant or understandable for consumers, and therefore these transparency requirements should take into account the different scenarios in scope of the regulation and be more flexible and less prescriptive. We also recommend clarifying Article 3 (2), as the current wording does not

specify who has the obligation to inform the customer about the scope, volume and purpose of data collection. It is not clear on which actor this obligation would fall, and it seems even conceivable that the retailer may be subject to this requirement in a B2C context, given the manufacturer will usually not be party to the purchase agreement.

These requirements could also **present significant challenges and barriers for design and innovation.** While companies will have an understanding of the intended use of the data generated, the nature and the volume at the design stage, they cannot anticipate these factors if the use of the product or related service changes, evolves, or adapts with evolving technology. It is not clear if that evolution in use would be permissible under the Act (whereas existing EU law provides for robust, risk-based, and principles-focused governance around such instances for personal data). It would also be important to ensure that this information can be provided digitally (e.g., via a QR code), to account for potential changes as devices develop/new services added for access.

We also note that throughout the Data Act, the use of terms such as "fair, reasonable and non-discriminatory terms" or "reasonable margin" as well as "where applicable" for technical requirements will lead to significant uncertainty. The application of such principles in the intellectual property space over the past decades, in particular for standard essential patents, has shown these are contentious.

Clarity with regard to article 4(6) would also be welcomed. In its current wording, the article seems to restrict the rights of the data holder to use the data to what has been agreed with the user of the connected device. This provision seems to be stricter than the regime introduced by GDPR for personal data, by excluding for example the possibility the use data on the basis of legitimate interest.

Finally, it would also be important to **clarify how the horizontal framework of Chapters 2 and 3 will apply to sectoral legislation**. While the Data Act proposal notes that future sectoral legislation should be "principle […] aligned with the horizontal principles of the Data Act," (p. 5), it is still unclear how/whether some of the principles of the Data Act will be applicable to the specific needs of some sectors. For example, in the MedTech industry, data are often collected solely for the purpose of obtaining, verifying and presenting data to clinicians, as part of the authorised intended use of the medical device. Providing access to such data outside this authorised setting for interpretation by a third party may create significant risks for patients' safety. This is in particular the case if the data were to be interpreted by a third-party device/software not subject to regulatory scrutiny under the Medical Devices Regulation. Similarly, the definition of user may be unclear as well, especially in the healthcare sector. Often a medical device is prescribed by a healthcare professional, worn by the patient (e.g., an implanted device) with the data accessible solely to the healthcare professional. It is unclear to what extent patient consent is required when the healthcare professional is requesting access to the data, or whether is it sufficient that the professional user is the data controller instructing the data holder, as data processor, to make the data available.

Considering the patient as user of the connected device may come with consequences not (yet) anticipated by the EU Data Act. For example, certain test results should not immediately become available to a patient without validation first by a healthcare professional, for example in the case of tests that are known to often provide false positives or negatives.

Build-in clear safeguards for companies' IP and trade secrets

To instill trust in a data sharing ecosystem, **it is important to ensure that commercially sensitive information is adequately protected.** The current proposal, rather than clarifying, creates ambiguity, whether protections for trade secrets are weakened. Disclosure of trade secrets and IP is of particular concern with the Data Act. Besides the provisions on the Database Directive in Chapter 10, on which we provide specific comments below, this concern manifests when assessing the potential impact of Chapters 2 and 3, especially given the broad access rights granted to users (art. 4), user-designated third parties (art.5) and other 'third-party-designated' third parties necessary to the provisions of a service requested by the user (art. 6(2c)). **Of particular concern is that the proposal does not include any protection of commercially confidential data, i.e., sensitive information beyond trade secrets,** whose sensitivity is for instance recognised in the Data Governance Act. More generally, to increase clarity of the framework of chapter 2 and 3, we suggest lawmakers strengthen the possibility for data holders to agree and apply safeguards to the use of the data made by users and third parties, especially when their commercial confidential data, trade secrets or IP are at risk of disclosure.

For the specific case of trade secrets, by requiring their disclosure, subject only to the recipient entering into confidentiality undertakings, **this Act does in fact fundamentally affect the existing rules on trade secrets.** Trade secret rights enable the protection of certain confidential information, but they also allow its exploitation. A trade secret holder can grant licences of its trade secret rights, including in return for royalties. Forcing holders of trade secrets to disclose them to parties not of their own choosing, subject only to the preservation of confidentiality, exposes the trade secret holder to increased risk that the trade secret protection may in fact be lost through a failure to maintain confidentiality, and undermines their existing rights in their information which they enjoy as a matter of European and national law. Furthermore, a mere undertaking to keep information confidential does not prevent that information being used against the interests of the trade secret holder.

According to Article 4(3) on the access rights for users, the data holder and the user can agree on measure for the protection of trade secrets, especially with regards to third-party access. Article 5(8) further specifies the safeguards against disclosure of trade secrets when a third party obtain access to the data. It says that trade secrets shall be disclosed to third parties "to the extent that they are strictly necessary to fulfil the purpose agreed between the user and the third party" and that the third party will have to put in place protective measures agreed with the data holder to preserve the confidentiality of the trade secrets. **These protections seem however insufficient, as companies would have limited oversight over the handling**

of their trade secrets and would have to rely on third parties to protect their business sensitive information. The insufficiency of these protection is more evident in article 11(2), which states that when a third party does use the data improperly, the third party should "destroy the data" (art. 11(2a)), and end production of any products and services developed "on the basis of knowledge obtained through such data" only where the data holder has suffered "significant harm" (art 11(3a)) and where such measure would be proportionate to the interest of the data holder (11(3b)). It is unclear how the concepts of significant harm and proportionality in article 11 would be defined in this context. The provisions here leave open the possibility for third parties to benefit from improper access to trade secrets and create significant uncertainty for companies who would risk having their trade secrets disclosed without having direct control over the types of protections applied. In complex IT systems with multiple IoT products from various providers, the provision also creates a risk of third-party trade secrets sharing.

Given that data holders and data recipients would have to negotiate a contractual agreement according to art. 8 of the Data Act, and that this agreement would not be binding if it "excludes the application of, derogates from or varies the effect of the user's rights under Chapter II," this uncertainty with regards to the protection of the data would lead to complexity and would make it difficult to reach an agreement between the two parties. It is also unclear what the legal consequences of a failure to agree between both parties would mean for the data transfer triggered by the user request. This protection of trade secrets is unlikely to work in practice, as governing agreements between data holders and their customers would have to define such data as trade secrets. Similar attempts to define such data in existing governing agreements have often been rejected by customers. As such, in this instance, customers are likely to also reject such claims of ownership by the data holder. **These concerns could be addressed by clarifying explicitly that there is no obligation to share trade secrets in relation to Chapter II**. Moreover, recitals 14 and 17 signal an intention to exclude data which is the result of processes which may be subject to intellectual property rights, or which is derived from data which represents the digitalisation of user actions. Therefore, we would argue that data which is the function of (sophisticated) processing or annotation, whether carried out within the device itself or after collection, should not be subject of obligations imposed by the Data Act. This would not prevent companies from sharing information confidentially if they choose to do so and the appropriate safeguards as they deem fit are in place.

A second concerning aspect regarding the **limitations for data recipients is the prohibition to develop a competing product for the user** (art. 4(4)) and for a third party (art. 6(2e)). Under EU competition law, the process of defining markets for competing products/services is very complex and often challenged in court. Using this unclear concept in day-to day data exchanges appears difficult. Also, once data is shared with a third party, data holders would have limited ability in practice to control of and insights into how the data is used (in particular to develop competing services), or what parties may access it further. **ITI recommends**

lawmakers to strengthen and further clarify this prohibition by giving data holders more control, as the current text does not sufficiently ensure that data holders are protected against their data being used to develop a competing product.

First, **it is unclear why the protection only covers "products" and thus excludes services** when the investment and R&D effort on the services side may in fact be significantly higher than for the product itself. This also ignores that monetisation is shifting towards the provision of services while products are increasingly commoditised. ITI is concerned that this may seriously undermine incentives to innovate and invest in this space.

Further**, it is unclear how these provisions would apply to dynamic scenarios,** for example when a product evolves in the future to incorporate new functions, which may become in competition with those developed by a user or third party at the time of their access to the data holder's data. Similarly, it is not clear if the data holder can refuse access to the data if a third party intends to develop a product which is in competition with other products that the data holder offers or intends to offer in the future, thus not in competition with the product from which the data originates. It also seems to ignore in-house development of competing product through reverse engineering which, although not aimed to create a competitive product sold on the market, would create a competition distortion.

Finally, **ITI recommends expanding the prohibition to develop a competing product also to *components* of products.** For example, whilst developing a competing robot or a vehicle, as products, would seem to be prohibited, the prohibition would not apply to developing a competing *machine vision component* when data from that vision component of the robot or vehicle are made accessible to the user or third parties.

The possibility to agree on the points above in a contract should be granted by the Data Act, to ensure that data holders can adequately safeguard their intellectual property.

Avoid Blanket Exclusion of DMA Gatekeepers

Articles 5(2) and 6(2d) also ban gatekeepers under the recently agreed upon **Digital Markets Act regulation** from benefitting from the data access rights introduced by the Data Act. We call on policymakers to avoid such blanket ban. In fact, **the provision ultimately limits consumer and business choices, creates complexity and limits the efficacy of the Data Act to facilitate data sharing**. The blanket ban of gatekeepers is against the logic of the DMA, which is based on carefully identified core platform services and addresses specific practices in very specific contexts. If the DMA designates a data holder as a gatekeeper, then there are regulatory obligations that kick in and competition law is still available to impose behavioural remedies to the extent the gatekeeper is found to be dominant and to abuse its market position. Excluding an entire undertaking from the possibility of being a data recipient is not necessary and excessive, especially when these are providers with a proven track record of developing products and services that consumers value and that benefit SMEs. Users may also be more willing to try new products and related services by porting the data to new entrants

in the space, if they are aware they have the possibility to go back to the original service provider in case they are not satisfied with the new products and related services used. The current mechanism fails to properly address any perceived market concerns and will likely lead to unwanted market distortions as end user choice is disproportionately restricted. Finally, it is also unclear how this provision would align with article 20 of the GDPR, that does not provide for such ban, and which can thus create conflicting requirements. This is especially since in the B2C context most data will anyway be personal data and, as a consequence, operators may merge Data Act and GDPR portability features in user interfaces.

Ensure coherence with existing legislative frameworks and industry best practices

It is also important that the proposal relies on global, industry-driven standards agreed upon in international standard development bodies for the most appropriate technical solutions to comply with regulatory requirements. The European Commission should also provide clear guidance on legal compliance, especially with the GDPR, which clearly exempts non-personal data from its scope on the basis that the privacy and data protection risk attached to that data is minimal, if a relevant consideration at all. The Data Act, and the Data Governance Act, will establish a governance framework for non-personal data that subjects non-personal data to many similar obligations without the benefit of the regulatory architecture that has built up around the GDPR, and how companies have invested (considerably) in order to comply. 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.

Existing best practices include 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 IoT area.

3. Unfair Contractual Terms – Chapter 4

Article 13 of the Data Act proposal aims to protect micro, small and medium-sized enterprises against unilaterally imposed unfair contractual terms concerning the access to and use of data, or the liability and available remedies in case of breach and termination of contract. ITI supports this objective and recognises the importance of ensuring that micro and SMEs are equipped with the necessary tools to participate in the data economy. It is however unclear how the SME status of a contractual partner could be reliably and continuously verified and the consequence of a change of this status for existing agreements. **It is also important to nuance key concepts like "unfair terms" and "unilaterally imposed terms" to ensure that the practical implementation of the bans is proportionate and workable.**

The specific instances where a contractual term is presumed unfair also require further definition. For example, point a) of article 13(4) is intended to protect against unfair terms that "inappropriately limit the remedies" in case of non-performance or breach of obligations. It is unclear, however, when a limitation of the remedies would be considered "inappropriate". Similarly, a clarification is needed regarding the concept of "reasonableness "introduced in point e) of the same paragraph. Additionally, a clarification that this provision does not apply to customary grounds for termination such as breach of contract, including non-payment, breach of the agreement, and other standard termination rights would be needed.

With regard to the provision of article 13(4)(c), it is worth noting that usage data, diagnostic data and application performance data may be generated by the user but are typically owned by the service provider. The language of the provision, stating that a contractual term shall be presumed as unfair when it prevents the party that contributed to or generated the data from using them, might make the rights of the service provider practically unenforceable.

It is also important to consider the volume of potential requests for negotiations of contracts that article 13 might create. Taking the example of a cloud provider that offers multi-tenant infrastructure, and whose services are not meant just for one or a few customers but for thousands of customers, it would be untenable from an economic perspective to negotiate each and every contract, especially given that every customer gets the exact same services, irrespective of their size. Furthermore, this might create tension with the requirements of article 8 which prohibits discrimination between comparable categories of data recipients.

It is generally accepted in Member States' contract law that a negative fact cannot be proven. It is indeed impossible for the party that supplies the terms and conditions to prove that the other party did not attempt to negotiate these. It is however fairly easy for the other party to prove that the unmodified terms apply, although it has sent a request for amendment. Article 13(5) should therefore be adapted accordingly.

4. Business-to-Government Data Sharing – Chapter 5

Chapter 5 requires data holders to make data available to public sector bodies upon request, when the public sector body demonstrates an exceptional need to use the data. The tech sector recognises the importance of timely access to data in emergency situations, where public bodies need to act fast to address an exceptional situation. The Data Act is well placed to harmonise the rules for data access and use in such situations at EU level, thus avoiding fragmented approaches between Member States and creating legal certainty for all actors involved.

Having said that, **requesting access to private sector data by public authorities should remain limited to exceptional and urgent circumstances, and accompanied by effective safeguards.** Requests should not go beyond what is strictly necessary to respond to the clearly

demonstrated exceptional need, either in time or in scope. In particular, we would encourage the co-legislators to consider the circumstances under which this is permitted currently under Art. 23 of GDPR. Additionally, companies that share data need to have sufficient assurances that their data, especially where they are business sensitive or entail intellectual property rights or trade secrets, are subject to appropriate technical and legal safeguards at least equivalent to those such companies apply. Furthermore, it would be important to clarify the scope of the provisions. Privacy and security considerations, as well as potential risks of data sharing for all actors involved, should also be taken into account. It is not in fact clear if the meaning of "data holder" in Chapter 5 continues to relate only to those entities that "through control of the technical design of the product and related services" are able to make available certain data, or if it extends to any data held by any entity.

Article 15 sets out the circumstances in which an exceptional need would be deemed to exist. Article 15(a) concerns responding to a public emergency, while 15(b) includes preventing and assisting the recovery from a public emergency. Article 15(c) allows public bodies to request data when this is necessary for fulfilling a legally mandated task in the public interest, specifying that a public body can make use of this provision only when it could not obtain the data by alternative means and the adoption of new legislative measures cannot ensure the timely availability of the data, or when this would substantively reduce the administrative burden for data holders or other enterprises. Aside from public emergencies which tend to be unforeseen and urgent, it is hard to understand what other circumstances would merit bypassing legislative action to invoke access to data. **More clarity is needed regarding the type of situations article 15(c) is aimed at that are not already covered by existing legal obligations to make data available.** This creates uncertainty and increases the risk of divergent interpretation across Member States and even between different public bodies in the same Member State.

According to the proposal, requests for access to data by public bodies must respect certain conditions, failing which the data holder may decline access or seek modification of the request. However, article 17(4) allows a public body that has obtained access pursuant to chapter 5, to share the data with another body. While in some cases this might be necessary and less burdensome for both public bodies and private actors, companies should be notified in advance and should have the possibility to express objections. This also goes with regard to the further use of data as per article 21. Here it is unclear how a "compatible purpose" would be defined. Additionally, data that contains confidential information or could give insights into proprietary technology should be excluded from the scope of article 21. We also recommend that article 17(2)(c) is amended to include commercially sensitive information (as do the Open Data Directive and the Data Governance Act).

Chapter 5 provides that data are made available for free when they are needed to respond to a public emergency (under art. 15(a)) and at technical costs for the other two cases (15(b) and 15(c)). **We suggest that policymakers focus on a balanced allocation of the technical costs**

involved with data access to be assessed on a case-by-case basis depending on the size and cost of the request. This assessment could also be undertaken once an emergency has ceased to exist.

Finally, questions further arise as to the rights of third parties whose data are held by companies that receive a government request. This could concern customer data of cloud service providers, digital platforms that have data about business users (e.g., e-commerce traders, independent drivers on mobility platforms or homeowners on flat sharing platforms) or even privileged data protected by professional secrecy. In all these cases, it is unclear whether these third parties should be informed, and to what extent they will have the right to an effective remedy, especially where decisions taken on the basis of these data may equally affect their rights.

5. Switching Between Data Processing Services and Interoperability - Chapters 6 and 8

ITI generally supports the objective to improve portability and switching between data processing service providers. ITI members have been active and supportive of industry-driven initiatives such as the codes on Switching Providers and Porting Data (SWIPO) to address the main obstacles to switching. **Switching is not a one step process and is not the sole responsibility of the originating data processing service provider.** While the porting out of data from a data processing service provider to a user is under the control of the existing cloud or data processing provider and can be handled by that provider (and generally the customer), this is not the case for switching. **Effective switching requires the co-operation of both the exporting and the importing data processing provider.** The Data Act, however, largely places the switching obligations on the exporting provider and creates obligations for incumbent data processing services providers to bear the responsibility of the switching process while ensuring full continuity of the services and functionalities under the same conditions. It is important to ensure that obligations on data processing service providers are proportionate and realistic. For this reason, we have many questions regarding how these provisions will work in practice.

As a general remark, it is fundamental that the obligations on data processing service providers in the Data Act reflect the different scenarios, including the variety of cloud services, the shared responsibilities between cloud providers and customers, data at play and their volume, the need to involve specific in-house or third-party technical assistance and the necessary costs that may arise, especially with complex switching projects. The Act must also tailor switching requirements to the sophistication of contracting parties and take into account market practices.

Many of the proposals in Chapter 6 are not appropriate for sophisticated B2B contracts. For example, the termination provision in Article 23.1(a) would effectively imply termination for convenience into every contract for data processing services and prohibit the parties from

agreeing to agreements with fixed terms. Many B2B data processing solutions have long deployment timelines, front-loaded implementation costs and other factors that require multi-year contractual commitments. **Termination for convenience upon 30 days' notice is extremely rare in these complex B2B solutions**, given the predictability that is required for these long-term arrangements, both from an operational and financial perspective. Introducing new termination rights into B2B data processing contracts by regulation would almost certainly lead to price increases and would be contrary to the expectations of B2B contracting parties. In addition, this goes against the existing financial model of several cloud providers that are publicly traded companies and have specific obligations vis-à-vis the stock exchange regulators relevant to how they recognise their revenue. There should thus be a clarification that this provision should not apply to contracts that are active on the day of the adoption of the Data Act, as this would have a considerable impact on the financial statements of several cloud providers. We suggest that lawmakers specify that the right to terminate within 30 days shall be granted to the customer when there has been a material breach of contract that the cloud provider has failed to remedy.

The obligations in chapter 6 to complete the switching process for data, metadata and applications **while ensuring service continuity and an equivalent minimum level of functionality** in the new environment (see definition of 'functional equivalence' in article 2(14)) **are not only out of current market standards, but also technically unrealistic and potentially problematic from a security point of view**. Even in traditional outsourcing contracts, which are always heavily negotiated because the service is customised to the user's needs, clients/users and providers agree on specific service level agreements that providers commit to meet during the termination assistance phase. 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 lifecycle of the contract. Parties also know that business and service continuity is better guaranteed through collaboration between both service providers and the client, rather than through simply transferring all obligations to the incumbent provider.

Especially concerning is the requirement of functional equivalence for Infrastructure-as-a-Service (IaaS) providers in article 26(1). Functional equivalence is defined in article 2(14) as a minimum level of functionality in the new environment to such extent that "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 the originating service at the time of termination of the contract." Cloud providers compete with each others and they offer different functionalities and different environments (i.e., a different customer experience). For this reason, functional equivalence would not always be possible. **It is impossible to envisage how the provider of the original environment can ensure that these minimum functionalities can be granted without having access to a competitor's environment, which will create security flaws.** In some instances, cloud providers provide services, for example communication with/surveillance of mobility devices, which are specifically tailored to a

customer's product, and which cannot function in other devices for security reasons. In these instances, providing functional equivalence would first not be possible with the products already placed in the market, and second, once included in the product offering, would lead to a significantly lower security level. The legislation must account for such cases.

Also, the **definition of 'the same service type' should be clarified** for example to account for cases where two cloud service providers have the same "primary objective" but achieve it in entirely different ways. The concept of "same service type" does not capture that two providers may have the same "primary objective" (e.g. database services), but go about achieving this in entirely different ways from an architectural and security perspective. The current approach of "functional equivalence" in the Data Act, would necessarily lead to homogenous/standardised service offerings which have a negative impact on service diversity among cloud service providers/customer choice and hence a damaging effect on competition. It could effectively create a "race to the bottom" for certain services while providing no tangible benefits for innovative services with no comparable equivalent. For example, a provider would be limited from bolstering a service's security if other providers could not provide that same heightened level of security through their own offering. A provider would likewise be unable to enhance the quality of its service unless there was some type of assurance that other providers could do the same. Finally, when a customer chooses a new provider, they may willingly decide to opt for different functionalities based on their own considerations (e.g., on prices or dissatisfaction with the incumbent) and therefore it is unclear why the original provider should ensure functional equivalence in these cases. To a minimum, we suggest lawmakers to better explain how this provision would work in practice and ensure that all parties in the switching process (original and new provider, customer) are involved to the extent that it is technically feasible.

Greater distinction could be made between infrastructure-level services (e.g. IaaS for cloud services), which are relatively standardised and commoditised, **and software services** which are higher up in the application stack (like PaaS or SaaS) and are more complex, often tailor-made, and which are not always perfectly interchangeable from one data processing service provider to another. Modern ICT applications are built on a rich and constantly evolving set of resources that offer choice in terms of capability, performance, cost, and other factors. Requiring all cloud service providers to use the same specific technologies or data formats would result in greater uniformity of software services that could lead to reduced choices for customers and likely impede the development of more innovative offerings in the EU. The proposal's focus on standards and formats does not sufficiently take into account that customers may choose particular standards and formats that make sense for their business and data service providers provide a vast array of options when choosing how to architect and run any given workload, including open source and proprietary options. Providers should be able to offer their customers the flexibility to adopt the specific combination of technologies as they see fit without being limited to particular standards and formats.

As mentioned, it is also important to recognise that different switching projects may require different time and budgets and that cost related to this operation is unavoidable, particularly when third party system integrators are involved. **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.** Data transfer fees are not meant to act as a disincentive to transfer data but reflect the cost of providing customers with network services. This includes the cost of network investments in equipment and network backbone (in addition to bandwidth) to provide a highly available, performant and redundant network that scales to customer workloads. The proposal does not consider that the cost and timing to switch to another provider is highly variable and depends on choices made by the customer, such as how the customer architected their solutions, what data the customer wants to move, what software the customer is using, the services on which the customer's solution is built, and the customer's destination solution. For this reason, **we are skeptical about the ambitious timeline of article 25 to phase out switching charges.** An alternative could be the clear scoping of what constitutes switching fees through transparent information on switching feasibility of particular services and pricing of any dedicated switching support services that can be provided at the customer's request, while leaving third parties the opportunity to provide switching services under commercial terms. Otherwise, the withdrawal of switching fees carries a risk of price increases for cloud services in Europe, which would in turn disincentivise cloud adoption. Mitigating potential switching costs is better achieved by good architecture, standard deployment practices, and pre-planning.

In order to recognise this complexity, **lawmakers should focus on clarifying/easing the strict deadlines of 30 days (art. 24(1a)) or 6 months in case of technical unfeasibility for completing the switching process**, and build more flexibility to allow providers and customers to complete the project in a timeline that takes into account several criteria such as the shared responsibilities in the switching process between incumbent provider, customer and new provider; developments and testing that are necessary; the volume of data to be switched; the legal and security requirements and the state of the art. In order to do so, it is important that contracts are terminated only at the end of the switching process, as opposed to the current language in art. 23(1a). Also, if a provider can prove that limited timelines for a migration process are "technically unfeasible" (art. 24.2), this process should be prolonged to the extent it would be technically feasible to migrate – in the interest of service and business continuity.

We also urge policymakers to **clarify which data would need to be ported to comply with the switching requirements in this Chapter.** For example, it is not clear if aggregate product usage data derived from user activity subject to the portability requirement. This seems both impractical and overbroad to the extent that data are blended with other users for purposes of product enhancement and learning. In addition, article 23(1c) mandates portability of applications and other digital assets, which is broad and unclear. The "application" portion of

this term, in particular, could be read to broaden the IP license grant of an application to extend beyond its original scope to use in third-party data processing environments.

Finally, we support the objective of Chapter 8 to support standardisation efforts in the field of interoperability**. It is fundamental however to ensure that processes to develop open interoperability specifications and standards on interoperability are based on participatory and industry-driven practices and takes into accounts proposed industry-driven specifications.** This is significant in the context of the Commission's new Standardisation Strategy and its review of EU Regulation 1025/2012, where we see a risk of reduced cooperation of EU standardisation bodies with international standardisation bodies. It risks setting multiple parallel standards that companies should adhere to but could also by design and/or by effect disadvantage non-EU companies, both generally and with respect to compliance with the Data Act. Developing workable interoperability standards should instead be subject to a multi-stakeholder global standard-setting process. Industry input is essential defining standards for particular data processing services, given the technical nature of these problems and the variability and dynamism of the data processing marketplace.

6. International Transfers of Non-Personal Data – Chapter 7

Chapter 7 of the Data Act proposal mandates providers of data processing services to take measures to prevent international transfer or governmental access to non-personal data when this would create a conflict with EU law or national law of a Member State**. ITI is strongly concerned with these provisions as they could unjustifiably restrict the ability of companies to transfer data across borders.** They could also be inconsistent with the EU's obligations under trade agreements such as the World Trade Organization General Agreement on Trade in Services. For various reasons, including the broad notion of "conflict" set out in Recital 77 and the lack of "derogations" to these data transfer restrictions similar to those set out in Article 49 of the GDPR, such provisions could create impediments to companies' ability to transfer non-personal data like (or potentially even greater than) those that the GDPR imposes on personal data.

Access to data is crucial for economic actors and beneficial to consumers around the world. It spurs innovation and is especially important to SMEs, allowing them to reach consumers and access new markets. **The flow of data across borders should thus be encouraged instead of restricted to support the global competitiveness of business in Europe.** We support the approach taken by the OECD in recommending the minimisation of restrictions on cross-border data access and sharing[1] and think that the provisions of Chapter 7 are contrary to this principle. Furthermore, negotiations on a new Trans-Atlantic Data Privacy Framework for personal data transfers are still ongoing. Creating a new legal regime for non-personal data transfers may limit the positive impact of the new framework for personal data transfers.

We also object to the manner in which Chapter 7 of the Data Act shifts responsibility for compliance with cross-border transfer restrictions from the customer to the service provider.

Customers of data processing services are the ones who control their data: practically this means that they know whether the nature of their data is subject to trade secrets, IPRs, national security schemes and other Union or Member State law. Customers are also the first target of judicial data request by non-EU judicial or administrative authorities. **IaaS or PaaS providers do not have the necessary means to determine which rules or legislation apply to the data they host and process, as these providers do not access these data,** neither do they know or can they anticipate the type of data that their customers will ask them to process during the performance of the services. Furthermore, under GDPR, data controllers are primarily responsible for ensuring that their cross-border data transfers comply with applicable laws. Of course, data processing service providers are responsible for fulfilling the data protection obligations established in customer contracts. Under the proposed framework, it is unclear what measures a data processing service provider should take to ensure compliance.

Moreover, from a policy perspective, it is important to consider that while restrictions to the transfer of personal data under the GDPR are motivated by a risk-based approach aimed at protecting fundamental rights, **non-personal data do not pose the same risks and are less likely to be subject to transfer or access request by third-country authorities**. Harms associated with access to non-personal data are not clearly articulated and ITI members note that government access requests to non-personal data are extremely infrequent and are even rare in the case of b2b cloud providers. Therefore, when considering measures that could create obstacles to international transfers of non-personal data, the Commission should adopt a risk-based approach, making sure such measures are clear and proportionate.

It is important to note that, both at international and European level, a number of instruments already exist to ensure the protection of certain rights in various contexts. As an example, intellectual property rights and trade secrets are protected through international agreements such as the TRIPS agreement or the Berne Convention. Other international texts deal with law enforcement access to data. It is unclear what added value the Data Act will have compared to existing instruments. On the other hand, it may create risks of overlaps and contribute to legal uncertainty.

Therefore, article 27 is neither proportionate to the objectives of protecting trade secrets and IP, nor justifiable. Concerns related to government access to data should be addressed through multilateral talks instead of sector-specific legislative requirements.

7. Implementation And Enforcement – Chapters 9 and 11

Member States will be responsible for the implementation and enforcement of the Data Act. They shall designate the authorities tasked with the enforcement and detail their powers and obligations. Levying fines for non-compliance with the provisions of the Data Act is also in the hands of the national enforcement authorities. This creates a risk of regulatory fragmentation and diverging practices across different Member States. Such divergences would defeat the

purpose of the Data Act, namely, to harmonise rules for data access and use within the European Union. **We would hence call for a European body to be responsible for official interpretation of the regulation**. Furthermore, it will also be important to ensure cooperation between different national authorities with the goal of a uniform implementation.

Lastly, we urge lawmakers to think of setting up a specific unit within the national Data Protection Authorities, that will deal with non-personal data sharing. This could be much more efficient than setting up separate bodies, because Data Protection Authorities will anyway be competent for all issues resulting from sharing mixed data sets.

The proposal confers on the Commission the task to develop and **recommend contractual terms on data access and use.** While these terms should remain voluntary, they could promote trust in data sharing, increase legal certainty, and become a valuable guidance tool for companies when drafting and negotiating contracts. The Commission should first consider fostering the use of existing data licensing agreements, such as the Community Data License Agreement (CDLA). In general, **we recommend that the Commission uses best practices that draw from experience and working methods established in other communities, such as the open-source community.** Community-led efforts in drafting and gathering feedback (e.g., via the Linux Foundation, Apache Foundation and Eclipse Foundation) and central administration of the licenses by the Open-Source Initiative have now resulted in a set of tried and trusted licenses that are widely used.

Then, should the Commission decide to develop these terms, these can only be designed and built in close cooperation with relevant stakeholders and in line with industry best practices, to make them future proof and ensure their wide adoption.

Finally, **we recommend extending the timeline for application of the Regulation.** The Data Act will set novel rules that will impact the design of products, set transparency requirements at points of sale and establish entirely new real-time data sharing request management systems that companies will have to continue to support. A period of three years, instead of the currently proposed one year, would allow companies to take the necessary measures to comply with the new requirements. Furthermore, a clarification that these new design and access requirements would only apply to products sold after the entry into force of the Regulation and not to products already on the market would be welcomed. Additionally, cloud service agreements currently in place do not take into account the proposed new switching rights and the proposed abolition of switching costs might have a significant negative financial impact on cloud service providers.

8. Sui Generis Right Under the Database Directive (1996/9/EC) – Chapter 10

We would welcome a clarification on whether the provision in article 35 applies to any databases containing data obtained from or generated by the use of a product, in all circumstances, or if it only applies to data holders in the context of the Data Act. Furthermore, more guidance is needed on the difference between collected and generated data, and how

databases should be designed and implemented to protect innovation, including incorporated trade secrets. The absence of clear guidance risks a stifling of innovation, particularly as sensors and other IoT devices incorporate AI and other technology advancements.