AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Data Act

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3.4 trillion in 2021, directly supports more than 4.9 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Executive Summary

The American Chamber of Commerce to the EU (AmCham EU) shares the objectives of the European Commission to increase data access and use through the proposed 'Data Act'. The Data Act should focus on promoting greater voluntary data sharing in order to boost economic growth, research and innovation, competitiveness, job creation, and to achieve Europe's digital transformation objectives. It should also ensure that international data flows are protected and encouraged, as they are not only vital to the European and global economy but also to the enhanced data sharing and re-use scenarios the Commission has identified.

In this context, the Commission should clarify the scope of non-personal data by distinguishing between data which is generated by a device or system, and that which is collected and stored. Technical advances in products today mean that some devices are not able to store, transmit and share all the data which is generated. Therefore, the provisions which mandate that all data generated must be collected and shared do not consider these more complex, technical devices. Acknowledging this distinction in the Data Act would enable sector-specific legislation to define the appropriate types of data which should be shared.

To ensure the Commission's data economy ambitions become a reality, AmCham EU believes that several aspects of the proposed Regulation require additional clarification. The new obligations should be clear, realistic, and balance the technical complexity of implementing new requirements with the need to foster user trust, serve customers' interests, and encourage the development of new innovative technologies and ways of leveraging data. The proposal should also recognize successful industry-led initiatives already underway which meet similar objectives, as many B2B and B2G data collaborations are already demonstrating the benefits that more open approaches to data can yield

Introduction

The Data Act, which complements the Data Governance Regulation proposed in November 2020 is the first deliverable under the European strategy for data. Overall, it aims to maximise the value of data in the economy, widening the data control of stakeholders, as well as its availability for innovative purposes. Indeed, Research indicates that the EU could be €2 trillion better off and gain two million jobs by the end of the Digital Decade if the power of international data transfers is fully harnessed and not stifled. However, the mandatory nature of certain requirements could have unintended consequences and risk disrupting existing and successful data sharing initiatives in Europe. Many existing business-to-business (B2B) and business-to-government (B2G) data collaborations, based on contractual freedom and the use of various data sharing technologies, provide important examples of the benefits that more open approaches to data can achieve. Potential restrictions on international data transfers, mandatory requirements on particular subsets of data, prescriptive portability requirements and lack of clarity on what type of data falls within the scope of the Data Act could all make collaboration more difficult. This is particularly case with international partners that are vital in tackling shared societal challenges and for companies operating globally.

Therefore, the Data Act should contribute to removing – not instituting – conflicts of laws and enabling – not restricting – the free flow of data. International data flows are indispensable for European companies' competitiveness, as they operate in a connected environment that goes beyond

the EU's borders. Regulatory policies should be developed in such a way as to ensure the principles of appropriateness and proportionality are respected and therefore avoid the risk of over-regulation.

International data flows

Article 27 of the draft Regulation places restrictions on the ability to transfer non-personal data outside the EU – including in response to a third-country government demand – when such a transfer (or access by third-country authorities) might give rise to a conflict with EU or Member State law. These provisions risk placing a disproportionate administrative burden on providers of data processing services, who are required to adopt all reasonable technical, legal and organisational measures to prevent international transfer or governmental access to non-personal data held in the EU. Given the overly broad notion of 'conflict' as set out in Recital 77, and due to the lack of guidance on European jurisprudence, these provisions could create legal uncertainty and impediments to companies' ability to transfer low risk non-personal data in addition to those that the General Data Protection Regulation (GDPR) imposes on personal data. Accordingly, article 27 risks creating a parallel personal data framework. It is also unclear how the Data Act would align with ongoing EU-US negotiations on international data transfers and how success on those fronts would be reflected in the Data Act.

Although cloud service providers may receive mandatory data transfer orders from third-country governments, non-personal data is less likely to be subject to access requests and does not raise the same kind of risks as personal data. The proposal itself seems to grapple with this issue as seen in article 27(3)(a), where one of the criteria to justify third-country access to non-personal data includes establishing a link to certain suspected persons - which *a priori* suggests the data will be personal. This could mean that deidentified, aggregated or anonymous data is no longer seen as an acceptable mitigation, regardless of the actual sensitivity of data in question. Additional guidance on the verification of a request which could fulfil the criteria in article 27(3)(a) will be developed by the Commission. It should be based on consultations with industry prior to the legal application of the Regulation.

Policy measures should therefore be sensitive to varying levels of risk presented by different types of data, with less restrictive measures governing lower risk data such as non-personal data. Exemptions where requirements can be waived should also be in place, for instance, in cases where countries already benefit from an adequacy decision from the EU. The proposal risks creating a situation, however, where cloud service customers, and regulators, focus on theoretical potential access which does meet the standards of Article 27 rather than whether non-personal data is the subject of requests in practice or actually presents a risk.

Finally, the requirement to be transparent about any data access requests that are received from third-country parties (article 27[5]) requires the provider to inform the data holder prior to disclosure. Given the 'data holder' refers to the entity with the obligation and ability to share data in the context of B2B/B2C and B2G data sharing, it would be more appropriate to refer to the customer of the data processing service provider.

Rather than imposing regulatory requirements on a specific sector, the Commission should solve issues around foreign authorities' access to data through multilateral governmental discussions. If such consensus cannot be found, the Commission should consider the adoption of voluntary guidelines (rather than regulatory intervention) to serve as a robust set of best practices laying a future-proof standard on law enforcement requests for data for data controllers and processors alike.

Any guidelines by the European Innovation Board should be developed in full and transparent consultation with industry. Indeed, industry's voice should be heard and taken into consideration, regardless of the origin of the company itself. In addition, any opinions given by competent bodies or authorities in regard to the conditions of transfers should be detailed, robust and timely.

Data sharing obligations

B2G

Business-to-Government (B2G) data sharing should remain voluntary. However, if mandatory obligations are adopted as proposed, 'exceptional need' should be more precisely defined, with corresponding use cases taken into account, and with proper safeguards in place for the sharing of personal and sensitive data. Aside from the provisions that refer to public emergencies (articles 15 [a] and [b]), which are by nature unforeseen and urgent, it would be important to understand which other circumstances would fall under a matter of public interest and mandate B2G data sharing.

Requests should also be limited to data sets that are already collected, aggregated and processed by the manufacturer, and shared with or accessible to third parties. They should not impact data which is processed solely on the device to support functionality between its components. For example, complex devices like automobiles have dozens of separate control units that interact to permit the vehicle to function; however, much of that data is only shared between the vehicle's subsystems and may not be collected by the manufacturer or even retained on the vehicle or component after use.

We welcome the provisions in the proposal which state that requests for B2G data must be limited, clear, explained, legal, legitimate, public, justified and not made available for a different use. However, data sharing should be limited to the public institution and not outsourced to third parties as such data could include sensitive information or give insights into proprietary technology. Sharing for a pre-defined purpose should be limited to the data collected by the business as part of their legitimate business practices and must not conflict with their legal requirements to delete certain data sets after a given period, under data retention legislation.

More clarity is also needed on the conditions that would grant access if 'the lack of available data prevents the body in question from fulfilling a specific task in the public interest' (article 15 [c]). There will be cost implications for the sharing of B2G data, especially when the request concerns personal data which must be anonymised and pseudonymised. Recovery of such costs should be recognised and guaranteed also in cases of public emergencies. The possibility to make data available for free should be left open to data holders as part of their crisis response strategy. Greater clarity is therefore needed on the threshold to be met in article 15(c)(1) where the public sector body 'has been unable to obtain such data by alternative means'. As a minimum, and in order to avoid public sector misuse of the corresponding provision, there should be some reference to a burden of proof that efforts have been made by public authorities to obtain the data through existing means. Failure to do so could lead to significant implications for existing B2G business models and in terms of privacy, intellectual property (IP) and trade secret protection and responsibilities. Moreover, claims of IP and trade secret protection by the data holder should require review and approval according to the appropriate standard.

B2C and B2B data sharing

Generated vs personal data

While the proposal's scope varies from chapter to chapter, the application to manufacturers of 'products' and providers of 'related services' of corresponding data sharing provisions remains broad. However, in a consumer internet of things (IoT) context, it is challenging to distinguish which 'generated data' would be personal data, and therefore already fall under GDPR rules. Draft data act sharing requirements go well beyond the GDPR portability requirements by forcing suppliers to make 'generated' non-personal content retrievable. Requirements to share non-personal data leads to an infinite scope, impossible to engineer, while bringing very limited added value to consumers. Such 'generated'" data could also include trade secrets and commercial confidential information. Thus, its protection should be made clearer throughout the proposal. For certain products, it is also often not possible to attribute data to only one user as a product may be used by more than one, making it difficult to identify the data consumer who would have the right to access data generated by the device.

The obligation to provide data in 'real time' is another practically difficult, if not impossible, provision to implement. In this way, a clear definition of what is meant by sharing data without 'undue delay' would be welcomed given the differing judicial practices in Member States. The meaning of 'where applicable' also remains unclear. We urge greater caution regarding the notion of 'real-time portability' in the context of IoT devices, which may implicate privacy and security concerns with respect to unauthorised access or other types of fraud. It would may also implicate data that could negatively impact the privacy of other users, as well as transparency assurances in how an individual's data is used. From a technical perspective, it would not be feasible to ensure the constant availability of all generated data from certain products. Firstly, the sheer amount of data would be significant in certain industries, particularly the automotive sector. Secondly, much of the data itself is not always available to the manufacturer and thirdly, the ecological costs could be significant given all the additional data that would then need to be stored.

Furthermore, while businesses who process personal data have experience presenting meaningful notices to consumers in compliance with data protection laws, the Data Act seems to require similar mechanisms for non-personal data as well. Given the lack of clarity around data scope and consumer value of these notices, the Commission risks mandating manufacturers to develop notices that are not meaningful to the consumer and do not achieve the stated transparency goals. It's unclear then what additional, and usable, data is targeted specifically in a B2C context. While it's clear that the 'publicly available electronic communication service' is the medium through which such data are transmitted, the definition of 'products' and 'related services' should be clarified to exclude electronic communication services and connectivity data from the scope of the data sharing obligations.

The lack of clarity on the scope of data covered and the players implicated also further complicates how the exercise of new user rights would work in practice, for B2C but particularly for B2B scenarios. Recitals 14 and 17 signal a clear intention to not cover data which is the result of processes that may be subject to IP rights, or that is derived from data representations in the digitalisation of user actions. This approach should also be reflected in the corresponding articles to ensure the scope of the data covered by the Act is clearly set out and limited to raw data which directly represents the actions of users.

Data holders

It is also unclear what role is expected of companies that would be considered data processors under the GDPR; are they, along with the manufacturer, also considered 'data holders' vis-à-vis end-users, or vis-à-vis the manufacturer (also generally considered a data holder)? This becomes even more confusing in B2B environments where many different platforms and services are implicated in complex ecosystems of 'products' and 'related services'. It is unclear whether a software developer who sells software for customers to implement in an IoT device would be considered a data holder just because they would have control over the technical design of a related service. In practice, the software developer is not generally entitled to access the data generated by the usage of an IoT device. Another example is IoT products which are powered by cloud services, considered as data processors under the GDPR. Customers are provided assurances, both contractually and technically, that they control their data. If such processors were to be considered as 'data holders' as per recital 21 – and hence subject to end-user requests without consent or instructions from the client user (the primary 'data holder') – the impacts on existing contracts and customer relationships would be significant and would require substantial renegotiations. It would therefore be important to clarify whether any user access requests, similar to GDPR, should be directed to the data controllers and, additionally, clarify what is expected in terms of compliance from companies traditionally considered data processors, particularly in B2B environments.

In general, setting different standards to define data holders for personal and non-personal data is not suitable nor justified. Therefore, recital 24, which equates the personal data holder to a data controller, and article 2(6) which considers as a non-personal data holder any entity that has 'technical control of the technical design of the product and related services', should use the same criteria. This will foster trust in data flows and in technology and will allow cloud vendors to implement the right safeguards to ensure that clients have control over their data (as required by recital 78).

Obligations of data holders

The Data Act outlines several obligations on data holders vis-à-vis their users before concluding a contract for the purchase, rent or lease of a product or a related service (article 3 (2)). However, it does not explicitly state to whom this obligation would apply (manufacturers, service providers or potentially to retailers) and would need to be further defined. Article 3(1) requires that covered products and related services be designed and manufactured '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'. However, it is not clear whether the obligation to make data accessible also means that data must be intelligible to users. If so, this also would need to be defined more clearly. Recital 18 indicates, for example, that the purpose of making data accessible is to allow users to 'make use of providers of repair and other services' and to allow businesses 'to launch innovative, more efficient and convenient services'. It may be that manufacturers are expected to provide data in a sufficiently readable format so that it can be used for at least such purposes. however, the Data Act contains no explicit provisions in this regard, creating additional confusion and implications for re-use. The readability requirement should exclude data that does not meet the requirements for mandatory sharing such as personal data or that related to IP, trade secrets or not deemed collectable. The Data Act is unclear regarding to which degree products and services already on the market would have to comply with these requirements, especially where technical limitations may make compliance overly burdensome or even impossible.

The underlying assumption of the data sharing provisions in articles 4 and 5 is that valuable data will be opened up for reuse by putting the user in control of access, use and sharing of data. Such a construct fails to recognise that in a B2B context there may be impediments to sharing data about the device in the other direction – from the user to the data holder. Access restrictions based on organisational administrative policy (eg maintenance window, remote access process, granting credentials) may impede delivery of after-sale services such as maintenance or analytics. While the user generally has an incentive to share the data, the move towards a remote work environment in a post-COVID world means these policies and processes are increasingly a barrier to providing the service.

Article 5(8) provides that as long as specific confidentiality measures are in place, the measures to preserve confidentiality under article 4(3) do not prohibit the user from sharing the trade secret with third parties if it is necessary to fulfil the purposes agreed between the user and third party. In effect, the confidentiality measures do not prohibit trade secrets from being shared both with users and third parties. Rather than focusing on confidentiality, the proposal should clearly exempt trade secrets from its scope (as stated above in the context of B2G) with an applicable reference to the Trade Secrets Directive, which should take precedence.

Article 4(4) and article 6(2)(e) state that the user and any third party with which they share the generated data cannot use such data to develop a product that competes with the one from which the data originates. These clauses are required because of the loose intellectual property protections in the draft proposal. This non-compete clause is very narrow as it only relates to a directly competitive product, not other products, services or processes, or even improving existing competing products already on the market. By undermining the usual means to protect data and adopting a narrow scope, it shifts the burden onto the data holder to demonstrate that not only has a trade secret been obtained and used, but that its use specifically breaches the non-compete clause, as well as making them responsible for investigation and enforcement. At minimum, the competent authorities' tasks (article 31) should explicitly include market surveillance and investigation of intellectual property and non-compete violations.

From a competition standpoint, the antitrust implications for companies complying with the Data Act's data sharing, portability and interoperability requirements raises some questions, particularly when it comes to the provisions of Article 5 on third party data sharing. Clarifications are needed as to what data a competitor might potentially have access to and how this interplays with the EU's competition rules, in particular 101 (1) of the Treaty. It is important to underline that if the information is commercially sensitive in so far as it is strategic, confidential and non-public, concerns future conduct regarding pricing or quantities. If itis information that relates to costs, output or capacity, investment plans, new technology or research plans, then it is particularly problematic. Hence, it is of utmost importance that the Data Act contains additional safeguards that would help strengthen the safeguards that should already be provided in the contract terms.

Article 5 stipulates that any gatekeepers designated under the yet to be adopted Digital Markets Act (DMA) are not eligible to receive data from users under the Act. The rationale for this significant regulatory intervention is unclear and the accompanying impact assessment remains silent on this point. The DMA was designed to address specific contestability issues for a set number of listed digital services. The carryover of the gatekeeper concept raises serious concerns since it bears no relationship to the market position of designated companies in the IoT field. In fact, it is conceivable that companies which, despite not being designated a DMA gatekeeper, have a strong market position in

IoT applications. This risks reducing competition. From a user perspective this rule arbitrarily limits choice of data which cannot be ported in case of a change of service provider, and limits a user's access to alternatives and re-use possibilities.

Scope & recital 15 exemptions

To ensure clarity, the exemptions in recital 15 should be referenced in the actual legal text (article 2[1)] and [2]). Products including, personal computers, printers and 3D printers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners, all of which require human input to produce various forms of content (eg, text documents, sounds files, video files, games and digital maps), should not be covered by this Regulation. This is because products which are primarily designed to display or play content, or to record and transmit content for the use by an online service, fall out of scope.

Additionally, the Data Act's horizontal approach should not conflict with existing and ongoing sectoral legislations on data sharing, which have been introduced as a result of EU legislative initiatives (eg in the health and payment sectors). As such, while Chapter 3 and 4 include general rules that should apply horizontally, Chapter 2 risks creating contradictory provisions by not explicitly excluding data sharing, which is already covered by existing sectoral legislation because of its specific nature.

Cloud portability and switching

The importance of data portability is well established and increasingly expected by customers. There is significant and increasing competition amongst providers to develop customer tools to better enable effective data portability across services. We support the Commission's ambition to make portability and switching easier, although many of the proposed rules seem difficult, if not impossible, to implement.

Data portability vs switchability

Data portability is different from switchability. While the porting out of data from a data processing provider to a user is under the control of the existing cloud or data processing provider and can be handled by that provider solely, this is not the case for switching, particularly if the innovative service used has no equivalence in the cloud market segment and/or depends on a level of assurance that cannot be maintained in a third-party cloud environment (e.g. third-party certifications). Effective switching requires the co-operation not only of both the exporting and importing data processing providers, but also that of the cloud user or customer. The Data Act, however, only places the switching obligations onto the exporting provider (articles 23, 26 and to a large extent 24). By comparison, the switching and portability obligations under article 106 of the European Electronic Communications Code (EECC Directive 2018/1972) are imposed on both the transferring provider and the receiving provider, as well as Member States. While the EECC scenarios are arguably far more straightforward than those in the cloud, they have nonetheless taken many years and significant investments to execute.

The proposal includes a general prohibition on 'obstacles' to switching, however, additional clarification is needed on the notion of 'obstacle' referred in article 23 (2). The Data Act does not provide a definition for 'obstacle', nor does it require that an obstacle meet a certain threshold of significance. As a result, it appears that virtually any commercial, technical, contractual or organisational factor – left to the discretion of the user - that might dissuade a customer from

switching services, could amount to a prohibited obstacle. This would create an impossible compliance obligation. It also negates customers choice on anticipating switching possibilities when opting for a particular data processing service.

Infrastructure-level services vs software services

Greater distinction could also be made between infrastructure-level services (eg Infrastructure as a Service (IaaS) for cloud services), which are relatively standardised and commoditised, and software services which are higher up in the application stack (like Platform as a Service (PaaS) or Software as a Service (SaaS)) and which are more complex, often tailor-made. Article 26 recognises a difference between IaaS providers, who are expected to ensure functional equivalence of the destination service after the 12-month compliance period, and PaaS/SaaS providers, who are expected to meet interoperability standards or specifications once they are identified and otherwise make open interfaces available and enable data portability. One issue of concern for the PaaS/SaaS providers is that it is not clear which interfaces are supposed to be available and how such functional equivalence requirements in the context of interoperability will work in practice.

More fundamentally, this provision does not line up with article 24(1)(a) which does not distinguish between different cloud services and requires all such services to allow customers to switch provider or port all data, applications and digital assets to an on-premise system. The technical feasibility clause here relates to their ability to complete as opposed to assist the switch, which does not respond to the question as to whether switching applications and assets is truly possible for the PaaS or SaaS service. Furthermore, even if open interfaces become available, there is an immense operational and technical burden required to switch between a cloud service and an on-premise service, as compared to switching between two cloud services. Cloud services are architected in an entirely different manner from on-premise services, such that re-writing them from scratch may be required to fulfil this requirement. Article 23 similarly fails to distinguish between IaaS and PaaS/SaaS, imposing portability requirements for applications and digital assets that may be bespoke to the service provider and therefore not reasonable to port.

Interoperability standards

Regardless of the fact the proposal allows for time to develop or identify interoperability standards or specifications to achieve switching at the level of 'functional equivalence' within the same service type for PaaS/ SaaS (article 29(1) and recital 72), the cost and feasibility of requiring that as a general principle seems to have been underestimated. 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. Recital 74 seems to guarantee that providers are not required to develop 'new categories of services' on the basis of the IT infrastructure of a different provider. However, it would be necessary to apply this requirement if the expectation is to port applications and digital assets (virtual machines, containers) to another provider or an on-premises system in a manner that ensures functional equivalence. Even cloud-native applications, which allow code to be run on different infrastructure stacks, may have dependencies in their operation. They may rely on back-end public cloud services, eg to validate the code, and have written specific scripts for that purpose which will not work when you change the underlying infrastructure. Relying on those back-end services, or building the whole SaaS service to a single IaaS provider's technology stack, reduces development cost and complexity. If a SaaS service has to remove existing dependencies, the costs can be exorbitant.

And if SaaS services need to be completely cloud-agnostic in the future, it also means they need to avoid using any new, innovative back-end services from the IaaS providers as they are not replicable on other platforms. Indeed, requiring all cloud service providers to use the same specific technologies or data formats would result in the uniformity of software services that could lead to reduced choices for customers and arguably impede the development of more innovative offerings.

The proposal suggests an unrealistic 30-day deadline (extendable to max 6 months) for switching, regardless of the volume and specifications of the workloads at hand. In practice, moving large amounts of workloads sitting across multiple hosting servers can be multi-year projects for the larger contracts. Particularly, in B2B contexts, switching projects will be more complex and will require more time than switching between consumer-facing cloud services (eg moving from a photo storage application to another). Additionally, in regulated industries cloud customers have very detailed exit plans agreed with their sectoral regulators. These cover several aspects of the switching process including timeframes. Imposing a horizontal obligation to complete the switching process in 30 days fails to take into account the technical and commercial reality of switching projects.

The prescriptive contractual requirements in articles 23 and 24 also go beyond what is reasonable in a B2B context. Some of these requirements could also lead to cost increases and a reduction of negotiating power for the cloud user. Article 23 (1) lays out a 30-day termination period which, along with a prohibition on switching charges (article 25 and 'obstacles', could impact the price reductions often common in longer-term (multi-year) contracts and arrangements, and in the wider ecosystem of third-party system integrators. Switching cloud services can differ significantly from a simple migration of stored data to free-of-charge portability operations under the GDPR. This relates to the variety of cloud services, the volume and complexity of data, the shared responsibilities between cloud providers and customers and the need for third-party specialist technical assistance and project management.

As the objective of this file is to enable switching between cloud, edge and other data processing services of the same service type, the proposal should exclude from these obligations those data processing services for which no equivalent services exist. Also, there may be data processing services operating on a trial basis or made available for free to test and evaluate businesses product offerings. These types of data processing services should be out of scope because they do not raise 'vendor lock-in' problems. Difficulties are likely to emerge regardless of defining what the 'same service type' is in the context of developing/identifying interoperability standards or specifications. Depending on how the concept of 'service type' is understood, there may be tens or hundreds of thousands of cloud service types in existence today. To serve as a useful construct for fostering switching opportunities, service types need to be narrowly defined and focussed on competing services that offer users the same basic functionality and the same service characteristics. While that may be better addressed in the standards development process rather than legislation, one guardrail that could be established would be the need to demonstrate that two services are actually competing for users before deciding they need to be interoperable for switching purposes. For example, SaaS services that only make sense within the environment of the vendor's own offerings – such as aggregating data from the various SaaS services of the vendor into a single platform for ease of operational orchestration by the customer. While other vendors may produce similar services that relate to their own offers, it is simply not relevant outside their own ecosystem, so while the service type is similar at face value, requiring them to be switchable is meaningless.

The notion of 'functional equivalence' should be clarified, if not removed altogether. Customers often choose their cloud service providers based on the special features that their services offer. It is impossible for data processing services to have adequate awareness of, let alone control over, the functionality and environment of other data processing services in order to ensure such functional equivalence. Furthermore, basing functional equivalence on a comparison of each output of a software system will necessarily drive towards monolithic system design where providers are incapable of differentiating their services because they must match every input and output – of which there may be hundreds of thousands or millions – with their competitors. Additionally, providers are not in a position to understand – much less track and adjust to – the performance, quality, and resilience of every competitor in the marketplace. Functional equivalence should either be removed altogether or re-focused to basic, comparable functionality offered by competing service providers without sacrificing either provider's security measures.

Specifically with respect to security, the obligation to support interfaces to facilitate interoperability must not have the side effect of requiring providers to make their services less secure or to alter their security properties to achieve different goals. If the open interoperability specifications that are developed do not support the security features of a particular provider, the provider should not be obligated to comply with the specifications and thereby sacrifice the provider's built-in security protections.

It is also worth recognising that even mandating the existence of interfaces that support switching may not be sufficient to cause switching or multi-cloud use to occur. Providers of today's cloud services have invested years' worth of engineering effort and resources to build the systems on the market today, and re-writing entire code bases in order to make use of new open interface specifications will likely be perceived to have a low return on investment in many cases where service design is already tightly coupled to the specific value-added services of an IaaS or PaaS provider.

Contractual fairness

The Data Act should ideally not impact existing contracts, nor should they impede members' ability to conduct business according to basic contractual freedom rules. Current provisions related to contractual terms could risk creating persistent ligation, with additional unfair burden placed on providers to prove terms have not been unilaterally imposed.

In this context, more clarity should be provided regarding 'good commercial practice in data access and use' and 'unilaterally imposed'. The lists of conduct that are always unfair and presumed unfair should be further specified to ensure legal certainty. Moreover, according to the proposal, the party that supplies the terms bears the burden of proof that they were not unilaterally imposed. This creates a presumption that is extremely difficult to overturn, given it is much easier to prove that a written attempt to negotiate took place than it is to prove that this has not happened. It should then be for the complainant to prove that the terms were nonetheless unilaterally imposed as a MSME is best placed to evidence that they unsuccessfully did attempt to negotiate terms (i.e. that the terms were unilaterally imposed).

Greater clarity is required regarding the respective rights and obligations of entities who may be holding data and receive a request to share data under the Data Act. The Act sets out some provisions

relating to rights that must be included in customer contracts, but data covered by the Data Act may be subject to multiple levels of contract rights that are not adequately addressed in the Data Act. For example, a natural person using a 'product' subject to the Data Act may do so in his or her personal capacity or as pursuant to an employment or other contractual relationship. Where the natural person is acting on behalf of another person pursuant to contract, presumably the Data Act rights in relation to relevant data will inure to the benefit of the employer or other person who contracted for the activity to be performed (and who may or may not be the owner of the product that generated the data). Similarly, data may be held by one or more entities on behalf of the data holder subject potentially to multiple levels of contractual rights, including obligations to safeguard data and to keep it confidential.

Enforcement and interaction with existing legislation

Consistency between the Data Act and other horizontal legislation will be necessary to create legal certainty and thus greater confidence in data sharing between businesses and across sectors (Data Governance Act [DGA], DMA, Digital Services Act [DSA], Free flow of Data Regulation, GDPR, as well as upcoming sectoral legislation including the European Health Data Space and access to in-vehicle data). The draft proposal references several of these legislations, which are in various stages of adoption, implementation and review. For example, it is disputable whether the Data Act proposal is in line with the DMA (a point the impact assessment also makes). The Data Act seeks to address perceived barriers to data-sharing by applying to a wider range of services of alleged 'gatekeepers'. This underlines that limiting data flows to companies that provide core platform services under the DMA is arbitrary. It is in the user's and wider ecosystem's interest to be able to freely choose a data recipient.

Additionally, the Data Act leaves significant discretion to Member States to designate competent authorities responsible for enforcement of different chapters and provisions. While additional powers and responsibilities will undoubtedly fall under the responsibility of EU data protection authorities, it is unclear to what degree this will be harmonised across Europe, particularly for those provisions and chapters where telecoms authorities or sectoral bodies may also have experience and competence. Moreover, there is potential for tension between the GDPR one-stop-shop mechanism (for personal data) and national enforcement (for non-personal data). Policymakers should strive for harmonisation in enforcement and competent authorities insofar as possible to provide businesses and customers with greater certainty on resources available for relevant guidance and regulatory feedback. For instance, the Data Act could institute a pan-European supervisory authority or a one-stop-mechanism and clarify how responsibilities will be allocated between data protection authorities and sectoral regulators when it comes to sharing mixed data sets within or between specific sectors.

The rights and obligations created by the Data Act also have implications under other bodies of EU law, such as competition and intellectual property law. For example, the Data Act would give users the right to require persons holding data generated by their activities to a third party , who may be a competitor of the data holder or others involved in its generation and use. The Data Act states that the recipient may not use the data to create a competing product, but how this safeguard can be implemented is unclear. Sharing competitively sensitive information may infringe EU and other antitrust rules. Although the Commission is working on revised guidelines to address the sharing of information and data among competitors under the EU competition rules, these guidelines do not address the interplay between the competition rules and new regulations, like the Data Act, that may mandate or seek to facilitate data sharing (not only among direct competitors but in potentially in

mixed horizontal and vertical contexts where the boundaries between competing products and services are unclear). These issues require further consideration and more detailed treatment both in the Data Act and in the Commission's competition policy guidance.

Similarly, data subject to the Data Act may involve intellectual property rights. The Data Act states that data holders will not be required to share trade secrets but it does not indicate how data holders can or must avoid sharing trade secrets associated with data covered by the Data Act. Again, these issues require further consideration and more detailed treatment.

Review of the database directive

The text under article 35 strikes an appropriate balance, as it aims to ensure IP protection for certain types of datasets while clarifying the scope and applicability of the *sui generis* right to align with the objectives of the overall proposal. In order to ensure clarity on the IP protection and to avoid confusion in implementing the Regulation, article 35 should be further aligned with recital 84 by specifying that the Database Directive does not apply unless the databases qualify for the *sui generis* right.

Other comments

Although the Data Act aims to capture situations when a user requests their data to be handed over to third parties (data recipients), the regulation does not explicitly mention that contracts between third parties and data holders without involvement of the user or third parties and users without the involvement of any data holder entity as defined is outside this legislation altogether. It is also unclear whether the collection of data by a third party from another third party authorised by the user could inadvertently be part of the scope. Those contracts are based on very specific objectives and would not fall under the intention of the Data Act.

In addition, it is not clear what happens when third parties process mixed data sets – eg raw data and processed data or collated raw data from multiple users (which could capture situations when there is a user request and situations when there is no user request). The regulation also does not allow the user to provide permissions for a third party to make use of the data outside of the regulation, even if they specifically wish to allow this. Such mixed data sets are not intended to be covered by the Data Act and further clarification is required. If such mixed data sets would fall under the scope, then this could require re-engineering of systems and processes to ensure data captured which falls in scope meets the obligations set out in article 6.

Conclusion

All in all, we support the objectives of the European Commission to increase data access and use through the proposed 'Data Act'. However, we believe that further clarification and work is needed in some parts. With this paper our goal is to contribute towards a more constructive, balanced and goal-oriented debate, in which industry's concerns and voices are heard and taken into account. In this way, we encourage policymakers to focus on the promotion of greater voluntary data sharing in order to boost economic growth, research and innovation, competitiveness, job creation, and to achieve Europe's digital transformation objectives. This can only be achieved if ensuring that international data flows are protected and encouraged, as they are not only vital to the European and global economy but also to the enhanced data sharing and re-use scenarios the Commission has identified.