BSA RECOMMENDATIONS ON THE EU DATA ACT

EXECUTIVE SUMMARY

BSA | The Software Alliance ("BSA")[1] is the leading advocate for the global software industry before governments and in the international marketplace.

Our members[2] are enterprise software companies that offer technology services that other organizations use—such as cloud storage services, customer relationship management software, and workplace collaboration software—to make their own operations more efficient, innovative, and successful. Increasingly, these organizations use BSA member services to generate value from data—to gain new insights from the data they hold, streamline supply chains, collaborate with partners, and serve their own customers more effectively.

In this context, BSA members are often neither the owner, nor the controller, of the data, but act as processors. It is their customers that own and control the data, while BSA members process and protect that data on their customers' instructions. This controller-processor relationship, pioneered in law by the European Union, is vital to the trust that customers place in BSA member companies and their offerings.

BSA welcomes the EU Commission's overall objective in its proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act, hereafter "Draft Proposal") "to unlock [the] potential of [data-driven innovation] by […] removing barriers to the development of the European data economy in compliance with European rules and fully respecting European values, and in line with the mission to reduce the digital divide". However, BSA would like to stress, as a preamble, that organizations that hold data— e.g. the customers that BSA member companies serve—should retain full control over whether they share or transfer data, to whom, and on what terms. Requiring organizations in the

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

[2] BSA's members include: Adobe, Akamai, Alteryx, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cisco, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

EU to share the non-personal data they own—or restricting them from sharing or transferring data, including across borders—will prevent EU organizations from taking full advantage of digital transformation, and will render them less able to innovate or compete effectively in global markets.

BSA recommends for the EU co-legislators to focus on the below objectives to ensure a balanced and effective Data Act:

- **Scope of the Regulation (Article 1) : Additional clarity as to the type of data covered**
- **B2B Data Access and Sharing (Article 2 (6) and Chapter II and III): Clarify the definition of data holder**
- **Unfair contractual terms(Chapter IV/Article 13): Ensure legal clarity in contract law**
- **B2G Data Access and Sharing (Chapter V): Clarify the concept of "exceptional need"**
- **Cloud switching (Chapter VI): the need to prevent anti-competitive behaviours**
- **International data access and transfer (art. 27): Refrain from imposing *de facto* restraints**
- **Interoperability (articles 28 to 30)**

1. Additional clarity as to the scope of the Regulation and the type of data covered (article 1)

Article 1§1 of the Draft Proposal stresses that the scope of the Regulation would pertain to a specific type of data, i.e. "data generated by the use of a product or related service". With regards the "product", Recital 14 (and article 2 (2)) provides further clarity as it stresses that it applies to connected/Internet of Things (IoT) products ("physical products that obtain, generate or collect, by means of their components, data concerning their performance, use or environment and that are able to communicate that data via a publicly available electronic communications service (often referred to as the Internet of Things)". Recital 14 also specifies that "the data represent the digitalization of user actions and events and should accordingly be accessible to the user, *while information derived or inferred from this data, where lawfully held, should not be considered within scope of this Regulation*" and Recital 17 further adds "… *such data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to IPRs*".

With regards "related services", article 2 (3) defines it as "a digital service, including software, which is incorporated in or inter-connected with a product in such a way that its absence would prevent the product from performing one of its functions". Finally, article 1 §3 specifies that the "protection of the provisions of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) supersede those of this Regulation".

Therefore, it appears that the "data" covered by the scope of the Regulation is only "raw" data generated by an IoT/connected product or related services, and only if it is non-personal data as such since, for personal data, GDPR takes precedence as provided in article 1 § 3 stated above. Finally, it appears, from the reading of Recital 17, to exclude those data which are the function of (sophisticated) processing or annotation, whether carried out within the product itself or after collection.

However, **chapters II and III pertaining to business-to-business (B2B) data sharing, chapter IV regarding data-related contractual terms, chapter V relating to business-to-government (B2G) data sharing and chapter VI on cloud switching** seem to entail a **broad range of data, i.e.** not just data generated from an IoT/connected product or related services but **potentially any business/commercial, non-personal data**.

Moreover, the assessment as to the distinction between personal and non-personal data will ultimately rely on the data holder and will prove burdensome to distinguish and isolate, as most data generated by an IoT products or related service often intrinsically have a personal component. Especially in a consumer IoT context, it remains unclear which 'generated data' would not be personal data already falling under GDPR rules.

BSA recommends that the Commission, the Parliament and the Council clarify the exact scope of the data covered by this Regulation to ensure that only "raw" data strictly generated from an IoT/connected product or related services is covered. While this clarification would not address the issue of whether the IoT data has a personal information component, and is therefore subject to the GDPR, it would address important issues of scope.

This is of **particular importance for article 35** which foresees that the ***sui generis* right** established **in the Database Directive 96/9/EC** does not apply to databases containing data obtained from or generated by the use of a product or related service. Indeed, a broad interpretation of the data covered would lead to a very limited, almost inexistent, protection of the right for developers or creators and therefore ultimately undermine the Database Directive and hamper EU innovation. Therefore, **BSA recommends narrowly defining the data covered by this Regulation** to ensure that it relates only to non-personal data strictly generated from an IoT/connected product or related services.

2. B2B Data Access and Sharing: Clarify the definition of 'data holder', as well as 'data user' in multiple relationships (Article 2 (6) and Chapter II and III)

a. Multiple data holders and users

The overall structure and provisions of the Draft Proposal seem to assume a one-to-one relationship between a data holder and a data user (with the possibility of the data user requesting the sharing of its data with a third party). The reality is more complicated, involving multiple companies. The Draft Proposal does not appear to provide a clear, predictable and legally certain answer to a situation where there are multiple relationships between data users and data holders.

In the case of multiple actors in a value chain, it could be argued that each company is, at some point in the line of relationships, both the data holder and the data user under the Regulation. This would trigger significant confusion between each of the companies and, ultimately, the final individual user, with regards the access and use of the data. Such multiple relationships trigger legitimate questions as to who the data holder and the data user is as well as, arguably, a complex and burdensome procedure for business and individuals to agree/request on sharing the data. This becomes even more confusing in B2B environments where many different platforms and services are implicated in complex ecosystems of "products" and "related services".

BSA would welcome **clarity as to the concepts of "data holder" and "data user" in such circumstances where there are multiple relationships**. In that regard, the GDPR has established **a well-functioning mechanism with the processor/controller distinction, whereby the data controller is the entity that "determines the purposes and means of the processing of personal data"[3] and the data processor is the entity that "processes personal data on behalf of the controller"[4].** Moreover, this could also be clarified by ensuring that parties can agree compliance obligations through contractual arrangements.

b. Data holders may be processors that do not have visibility into the data

The Commission's proposal in article 2 (6) defines the "data holder" as "a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable

[3] Art. 4(7) of the EU General Data Protection Regulation
[4] Art. 4(8) of the EU General Data Protection Regulation

Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data".

BSA believe this definition creates confusion, notably with regards the B2B and B2G data access and sharing, as it seems based on the false premise that technical design of a related service induces control on the product generated data.

Indeed, BSA members are B2B companies whose customers are generally businesses that own and control the data. In the context of cloud services, for example, business customers are provided assurances, both contractually and technically, that they own and control their data. A concrete example would be the software developer that sells the software to its business customers who then implements it in an IoT device. In this context, BSA members are often neither the owner, nor the controller, of the data, but act as processors. It is their customers that own and control the data, while BSA members process and protect that data on their customers' instructions. Therefore, BSA members (cloud service providers), if qualified as "data holders" under the present Draft Proposal, would then be required to share data they may not have access to or are prohibited from viewing by contractual obligations with the actual controller of the data, their business customer, which owns and controls them. In case of complex datasets which could include third-party data (such as customer's providers, sub-contractors, etc.) and for which there is no direct contractual relation with the related service provider, it is even more problematic for them to be put in such a position. Moreover, this obligation may also be inconsistent with the role of processors under GDPR, because requiring processor to identify data sets to be shared and the parties with which they should be shared may constitute determinations about the "purpose and means of processing," which are left to controllers under GDPR.

Deferring to contractual agreements between the controller and processor would better align with the stipulation in Recital 24 that "this Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder". Therefore, any request to BSA member companies would often render compliance by such companies impossible for technical or contractual reasons, since such companies are not in direct contact or relationship with the user and cannot, as such, access the user's data to comply with the request, or have contractually committed to act as processors rather than controllers under GDPR.

A broad interpretation of "data holder" that extends to companies acting as processors would inadvertently undermine the GDPR's GDPR's **well-functioning mechanism with the processor/controller distinction. Under that distinction, the data controller is the entity that "determines the purposes and means of the processing of personal data"[5] and the data processor is the entity that "processes personal data on behalf of the controller"[6].** Recital 5 seems to allude and recognize such distinction since it stresses that the Regulation "*takes as its starting point the control that the data holder effectively enjoys, de facto or de jure, over data generated by products or related services*" but Recital 21 creates additional confusion as it provides that "the server may be the

[5] Art. 4(7) of the EU General Data Protection Regulation
[6] Art. 4(8) of the EU General Data Protection Regulation

manufacturer's own local server capacity or that of a third party or a cloud service provider who functions as data holder".

We **recommend that the co-legislators**, taking into account the existing distinction contained in the GDPR, **clarify that, only business customers, i.e. companies that own and control the data, be defined as "data holders"**. Companies that merely process the data, but do not have ownership or control over the data, should not qualify as "data holders", and should therefore not be subject directly to such provisions.

c. Protecting Trade Secrets

Moreover, some BSA member companies develop and deploy industrial IoT applications (in industries ranging from healthcare to manufacturing, automated or connected vehicles, and even for the operation of the International Space Station). The B2B data accessibility and data sharing provisions as laid down in Chapter II and III intend to open valuable data 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 also 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 (e.g. 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.

More significantly, these provisions are likely to create serious issues related to intellectual property (and trade secrets) and commercial law, as well as to the security of the affected software (making the data available to all users and the third-parties they select could severely weaken the resilience of the software product), and severely affect their ability to freely develop their software based on customer demand and technological excellence. In that regard, the mere mention, in Recital 28, that "any trade secrets or intellectual property rights should be respected in handling the data" and Art. 4 §3 that "trade secrets shall only be disclosed to the user provided that all specific necessary measures are taken by the user to preserve the confidentiality of the trade secret especially in relation to third parties", appears too little and too vague to ensure that IP and trade secrets of EU companies are protected. Indeed, in a B2B relation, using the controller/processor distinction laid out above, our members companies (data processors) could be required to provide access to data of their business customers (data holders/controllers) which may be protected by IP or trade secrets. Article 5 §8 goes on to state that if 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 focus on confidentiality, the proposal should clearly exempt trade secrets from its scope. Art. 4 §4 introduce some limits on use of the shared data insofar as "the user shall not use the data (…) to develop a product that competes with the product from which the data originate" and this is reinforced in Art. 6 §2(e). However, this non-compete clause is very narrow as it only relating 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 also 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.

Moreover, and surprisingly, this proposal ignores "commercially confidential data" whilst the Data Governance Act included it (alongside trade secrets and other IPRs). Not all sensible data raises to the level of a trade secret, however they still merit protection.

Furthermore, the Explanatory Memorandum to this Act clarifies that "this proposal does not affect existing rules in the areas of intellectual property (except the application of the sui generis right of the Database Directive)… or the legal protection of trade secrets." However, by requiring the disclosure of trade secrets, subject only to the recipient entering into confidentiality undertakings, this proposal 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, nor does it suffice to prevent any competition disruption on a market due to such a disclosure.

BSA would recommend therefore to exclude any confidential business/commercial data from the scope of the B2B and B2G Chapters in order to guarantee both the safety, security and IPR protection, or, at the very least, that its access and use conditions be agreed upon by the data holder and the user. Additionally, for cases where the access to data could create additional security risks (for instance where the data could be used to reverse engineer the security controls), a limitation for making the data accessible should be also foreseen.

3. Unfair contractual terms (Chapter IV/Article 13): Ensure legal clarity in contract law

In Chapter IV (article 13), the Commission addresses unfairness of contractual terms in data sharing contracts between businesses, in situations where a contractual term is unilaterally imposed by one party on a micro, small or medium-sized enterprise.

As a preliminary comment, we would like to stress that freedom of contracts is a fundamental principle of EU law and protected by Member States' national laws. Increasing trust in data sharing is essential, yet B2B data sharing models already exist and yield successful results that demonstrate what can be achieved when trust is established between collaboration partners with contractual freedom. The Data Act should not disrupt such models, but rather aim to provide European businesses with the ability to choose among the widest range of data sharing mechanisms and contractual models that exist in the market, as different use scenarios may require different features (level of protection, access restrictions, etc.).

First, we read the prohibition of unfairness of contractual terms in this Chapter as applying beyond "data sharing contracts", to any terms contained in a contract that relate to access to and use of data. Indeed, this reference to "data sharing" could be read more narrowly than the Act itself suggests – that is, the chapter could impact a wide variety of business contracts where data is provided or made available by one counterparty to the other, even where the provision of that data is only a minor aspect of the contract (e.g. common contractual clauses such as delivery of materials/information upon or after termination).

Second, there appears to be a tension between the requirements on non-discriminatory terms (Article 8) which should be always met by data holders and the requirements of Article 13 that data holders do not unilaterally impose terms on micro/SMEs and make changes to standard terms if those are requested by a micro/SME – if these are not to be considered as unilaterally imposing a term.

Finally, we believe the Draft Proposal appears too general and vague in the concepts used to define such "unfair" terms, especially when using provisions such as "grossly deviates from good commercial practice in data access and use", or "contrary to good faith and fair dealing" (article 13 (2)). **BSA cautions that such broad concepts lack the legal clarity and certainty needed in contract law and will therefore likely increase the risk of litigation leading to different results**. At the very least, any bans should be proportionate and limited to clearly harmful practices, rather than potentially disrupting contractual freedom and legitimate legal protections for service providers. In particular, without a common understanding of "fairness" (or "unfair terms", or the above-mentioned concepts) in contracts across the EU, courts and competent authorities will need to step in at the national level to interpret and ultimately define such concepts. It may also lead, through differing interpretations at Member-States' level, possibly further fragmenting the Digital Single Market.

Furthermore, 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. We would therefore recommend that Article 13 §5 be adapted accordingly.

4. B2G Data Access and Sharing (Chapter V): Clarify the concept of "exceptional need"

BSA recognizes the value that can benefit society when private- and public-sector entities share data with one another. Indeed, and in particular over the last years, BSA members have been working closely with European governments and public-sector organizations to use and share data to respond to the COVID-19 pandemic, including to create data maps to track the spread of COVID-19 and to forecast needs for hospital beds and testing in at-risk regions.

In these and other scenarios, BSA members have found innovative ways to share data and collaborate with governments for public-interest purposes without the need for data-sharing mandates. In this regard, in June 2020, BSA has launched its Open Data Agenda to help advance responsible policies that facilitate greater sharing, collaboration, and

experimentation with data resources while protecting privacy. We continue to support such voluntary efforts. Accordingly, **BSA would encourage that the Draft Proposal focuses first and foremost on facilitating voluntary data sharing between private- and public-sector entities,** such as by offering model contractual terms for such agreements and providing assurances that private-sector entities that do share data will be fairly compensated, as appropriate.

If the Commission and co-legislators were to favor, as it is the case in the Draft proposal, such B2G data-sharing mandate, BSA would strongly recommend the following:

1. First, since the concept of "exceptional need" is the cornerstone principle for the B2G data sharing, and where rights are granted for public sector to access privately-held data on that basis, **the "exceptional need" element** must be carefully balanced against the costs and risks this may entail. Indeed, aside from public emergencies (Art 15 a and b) which tend to be unforeseen and urgent, it is hard to understand what other circumstances would merit bypass legislative action to invoke access to data. Moreover, such a possibility could constitute a disincentive for public authorities to seek a legislative route to address future requests for data. This concept is too **quite broad and vague and such access should then rather be limited to the "public emergencies" circumstances foreseen in Article 15 a) and b). However, if the concept of "exceptional need" were to remain, we believe that, at** the very least, there should **some reference to a burden of proof that such efforts have been made in order to avoid public sector misuse of the provision**, which could lead to significant implications in terms of privacy, IP and trade secret protection and responsibilities.
2. Second, **such data-sharing obligations should be directed at the entity that owns and controls the data**. Indeed, as noted earlier, companies processing data should not be forced to share their customers' data with public-sector authorities, certainly not without their customers' knowledge or consent. Forcing data processors to share the data of their data-controller customers would likely violate these processors' contractual obligations to customers might conflict with requirements under other EU or Member State laws, and will undermine trust in technology and digital transformation across industries.
3. Third, and regardless of point 1 above, BSA would recommend **providing compensation** for both cases, i.e. "exceptional need to respond to public emergency" (art. 15 a)) and "other cases of exceptional need" (art. 15 b) and c)), and not only for b) and c).
4. Finally, and in line with the Commission's rationale on article 27 with regards international transfer and access of data, **any B2G data-sharing obligations should be limited to data that is owned or controlled by an entity established in the EU**. Forcing companies to share data owned or held in jurisdictions outside the EU, for the benefit of a public-sector entity in the EU (and not for well-recognized interests such as fighting terrorism or crime), could violate third-country law, which in turn might invite retaliation by foreign governments or place private-sector entities in unavoidable conflict-of-law situations.

5. Cloud switching (Chapter VI): the need to prevent anti-competitive behaviours

BSA supports data portability. Business customers of BSA member services are generally free to decide what data they wish to store or process in the service, and can remove that data at any time. Also, most BSA members offer tools that their customers can use to facilitate the porting/switching of their data into and out of the service, in many cases using widely-used machine-readable formats if the end customers/users wish to do so. Portability for personal data is also a right guaranteed by article 20 of the GDPR, which the Regulation rightfully mentions. In a B2B environment, cloud providers are generally acting as processors and thus are not in a position to make decisions about whether to port particular data sets. Those determinations are appropriately made by the business customers using cloud services, i.e. controllers or data holders. Given that many cloud systems hold a broad range of information, including both personal and non-personal data, portability is often offered to business customers for all the data they have in the cloud provider's systems, irrespective of whether these data are personal or non-personal. Moreover, 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 solely by that provider, this is not the case for switching. Effective switching requires the co-operation of both the exporting and the importing data processing provider. The Draft Proposal, however, solely places the switching obligations on the exporting provider.

The market for enterprise cloud services already provides numerous options and best practices (e.g. the SWIPO Code of Conduct – see below), developed by the businesses dealing with the issues, based on the experience of the market and the practical needs of customers that want the ability to port their data into and out of the service. We understand that the issue the EU Commission is trying to tackle is the "vendor lock-in" which is precisely what the SWIPO Code of conduct is designed to address[7].

BSA would therefore strongly encourage the Commission, Parliament and Council to support ongoing industry efforts, such as through those industry codes of conduct, such as the SWIPO Code of Code of Conduct, already aiming at facilitating portability and switching. The SWIPO code was established rather recently, and the Commission should, in the first instance, further encourage and support this initiative to gather more trust and awareness in the market (for instance by including it in the upcoming EU Cloud Rulebook), assess whether it is applied and addresses the concerns, notably the "vendor lock-in", instead of considering legislating on portability/switching at this stage already.

However, BSA welcomes the fact that the EU Commission, in its draft proposal, chose not to impose any technological mandate. Indeed, Cloud services compete not just on price, but also on the features and technology choices they offer to their customers. Requiring all cloud service providers to use a single set of mandated technologies or data formats would lead to reduced choices for customers and impede innovation. Nonetheless, the

[7] "*The European Commission wants to avoid vendor lock-in and create a competitive European digital market where it must be easy to switch from provider, including the porting of business data involved*", Introduction to the SWIPO Code Of Conduct, SWIPO-Codes-of-Conduct-Common-high-level-principles.pdf, p.3.

cost and feasibility of requiring switching at a level of 'functional equivalence' within the 'same service type' as a general principle seems to have been underestimated.

"Functional equivalence", as described by Articles 26.1 and 2(14), includes an obligation for the incumbent provide to "***ensure***" "the maintenance of a minimum level of functionality ***in the environment of a new data processing service after the switching process***. This obligation rises to such an extent that, in response to an input action by the user on core elements of the service, the destination service will deliver the same output at the ***same performance*** and with the ***same level of security***, ***operational resilience*** and ***quality of service*** as the originating service at the time of termination of the contract". This also leads to technical and operational difficulties, notably for Infrastructure as a Service (IaaS) cloud service providers. Indeed, there is a lack of legal clarity as to what, concretely is expected from the incumbent cloud service provider to guarantee such functional equivalence, in particular in terms of ensuring the same level of security and performance, let alone the quality of service and same output, ***in the environment of one of its competitors***. If such equivalence implies for the incumbent cloud service provider to have access to another other cloud service provider's environment, the new provider will face security issues if its competitor can access its own environment. Also, if the new provider does not provide the same level of security, resilience, service quality or performance, there are outstanding questions as to whether the incumbent provider should step-in since there appears no other way for it to otherwise comply with its statutory obligations under Article 26.1 and prevent liability claims.

Greater distinction could also be made between Infrastructure as a Service (IaaS), and software services which are higher up in the application stack (like PaaS or SaaS), more complex, often tailor-made, and which are not always perfectly interchangeable from one data processing provider to another. While the proposal recognizes such a distinction, the difference in expectations becomes less clear with "functional continuity" requirements referenced in the interoperability provisions (articles 28 to 30). Imposing "switchability" requirements (whether in the context of portability or interoperability) for SaaS/PaaS services so that all services are interchangeable or mandating technical specifications and/or a fixed set of common denominator functionality, would in practice result in requiring all services to be effectively identical. This would lead to a loss of innovation capacities for European companies and users. It also disregards the complexity and singularity of customers' strategic choices in building their IT systems, associating, at will, various software layers.

Moreover, the obligation for a Cloud service provider to ensure service continuity in Article 24(1)a(2) is concerning as it is unbalanced and unrealistic. Even in traditional outsourcing contracts, which are heavily negotiated, clients/users and providers agree on specific service level agreements that providers are bound to comply with during the termination assistance phase, where providers transition clients' workloads to another provider. The service levels agreed therein never foresee a 100% service continuity, as parties understand and agree that the service will not be the same during a termination phase as during the lifecycle of the contract. Parties also know that business and service continuity is better guaranteed through collaboration between the service provider and the client, rather than through shifting obligations on the provider.

In addition, the prescriptive contractual requirements in Articles 23 and 24 also go beyond what is reasonable and common practices in a B2B (and even B2C) context. Some of

these requirements would also likely lead to cost increases for the user. Article 23 (1) lays out a 30-day termination period which, along with a prohibition on switching charges (Article 25), could impact price reductions often common in longer-term (multi-year) contracts and arrangements. No possibility is provided for data processing services to recuperate such costs, yet this should be considered and addressed in the proposal.

Indeed, with regards Article 23 (1a) mentioned above, we are concerned about the inclusion of a termination notice period of maximum 30 days that would allow the customer to terminate their contract, at any given moment in time and for any reason. Such a requirement would have a disproportionately disruptive impact on a large number of cloud providers who operate on a subscription-based model, as the customers would be able to terminate their contracts at any moment and even with no reason, making it impossible for a company to calculate its revenue for the next six months or the year. . It also disrupt the overall balance of many cloud ecosystem operators, such as integrators, sub-contractors, etc. This negative impact can be mitigated by introducing a provision clarifying that: a) the customer should provide its termination notice *minimum* 30 days before the switching process can start, to allow the incumbent provider to prepare a successful switching process, and b) a right to terminate the contract in 30 days shall be granted to the customer in case of material breaches of the contract that the cloud provider has not tried to remedy. Finally, if a provider can prove that limited migration timelines are "technically unfeasible", these timelines should be prolonged to the extent it would be technically feasible to migrate (Art. 24.2). This is beneficial both to service and business continuity.

Finally, BSA would welcome additional clarity as to what "commercial, technical, contractual and organisational obstacles" (Art. 23 (1)) providers of data sharing services should remove, entails in practice. Indeed, it appears that virtually any commercial, technical, contractual or organizational factor – left to the discretion of the user - that might dissuade an enterprise customer from switching services could amount to a prohibited obstacle. This would create an impossible compliance obligation. One such example would be to know how the cloud service provider would address the situation where an open standard arises between the conception of the initial service and the switching. Another example of such obstacles could be fixed term contracts (that customers select because of the discounts these entail). According to Article 23.1(a), these well-established and generally accepted commercial covenants would be seen as a contractual obstacle to terminate the contract after a 30 day-notice.

6. International data access and transfer (art. 27): Refrain from imposing *de facto* restraints

The Draft proposal offers specific safeguards, by way of providers having to take "all reasonable technical, legal and organizational measures" to prevent third party access to non-personal data held in the Union that conflicts with competing obligations to protect such data under EU law, unless strict due process conditions are met. Moreover, the explanatory memorandum of the proposal specifically stresses that "the Regulation complies with the Union's international commitments in the WTO and in bilateral trade agreements".

It appears that article 27, paragraph 1 allows data transfers from one company based in the EU to another based outside the EU, provided the company based in the EU takes "all reasonable technical, legal and organisational measures, including contractual arrangements, in order to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law or the national law of the relevant Member State". Paragraphs 2 to 5 of article 27 apply to B2G international data transfer, i.e. the sharing of data by a company based in the EU to a government of a country located outside the EU. Such B2G international data transfers could only take place under the conditions laid out in those paragraph 2 to 5 (international agreement, judgment, etc.).

The requirements of paragraphs 2 to 5 appear tailored in a manner that create safeguards but allows, for instance, law enforcement access with sufficient due process considerations. BSA encourages the co-legislators to clarify this understanding of article 27, and ensure predictability and legal clarity, in particular on how the rules are going to be enforced, as well as to what will be the criteria to determine whether the measures taken comply with the law.

Companies may not be aware of which process foreign governments may use to request data. Hence, BSA would like to reiterate that any concerns about foreign government access to data should be addressed through multilateral governmental negotiations.

Unnecessary restrictions on the freedom of companies to transfer data across borders would jeopardize digital transformation and cybersecurity. As the OECD has noted, "[*d]igital technologies and data profoundly affect international trade by reducing trade costs; facilitating the coordination of global value chains; diffusing ideas and technologies across borders; and connecting greater numbers of businesses and consumers globally*."[8]

The services that BSA members offer their enterprise customers help them connect, collaborate, and innovate across borders, and thereby to participate fully in the global economy. And companies from all sizes and in all sectors rely on the ability to transfer data around the world to innovate and create jobs[9]. Any restrictions on such transfers should therefore be limited to what is strictly necessary to serve a legitimate public interest, be limited to the least trade-restrictive option available, and not be imposed on a specific sector. They should also specifically not impinge on the free flow of cross-border non-personal data necessary to ensure adequate levels of protection against cyber-attacks, a threat of global nature. The provisions of article 27 (paragraphs 2 and 3) of the Draft proposal fail to meet this standard. The Commission has come forward with no evidence to suggest that third-country law enforcement requests for data (or indeed requests from any other third-country authorities) pose risks to EU organizations' IP rights in their non-personal data, or otherwise are preventing them from commercializing or otherwise exploiting that data. Moreover, it is exceedingly unlikely that law enforcement demands for *non-personal* data will infringe upon fundamental rights set out in the Charter. Lastly, not all providers receive the same amount of government requests, in fact B2B providers often receive very limited requests due to the nature of the services they offer. B2B service providers are not even the first addressed in such a request, rather their business

customers are. Absent such risks, the rationale for the Commission's data transfer restrictions for non-personal data are difficult to discern. Therefore, we would urge that any policy options related to government access to non-personal data issues in the international sphere should ensure a level-playing field, be proportionate to the risks, and be non-discriminatory.

Moreover, given for that the rationale for introducing these requirements is to protect non-personal data of sensitive commercial, national security or defense value, the broad application of these provisions to all non-personal data and its likely consequence seems extraordinarily heavy-handed.

The impact for business on these provisions is likely to be significant. While a request for non-personal data is rare, the concern is that cloud service customers and regulators are going to be focused on whether the cloud service provider could *theoretically* be subject to a legislative instrument that does not meet the standards of Article 27 rather than whether non-personal data is the subject of requests *in practice or actually presents a risk*. This could mean that deidentified, aggregated or anonymous data is no longer seen as acceptable mitigation, regardless of the actual sensitivity of data in question.

An additional point relating to the requirement to be transparent about any requests that are received (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 is confusing to use this term in the context of government access to data. It would be more appropriate to refer to the customer of the data processing service provider. **We also urge the Commission to ensure that the Draft Proposal is fully consistent with the EU's broader commitment to free and fair trade,** and to consider whether the language as proposed is fully consistent with the EU's commitments under the WTO General Agreement on Trade in Services (GATS) and other trade commitments. Finally, we are certain that the Commission would wish to avoid imposing rules with regard to foreign authorities that authorities in the EU could not themselves comply with. Indeed, if a third country were to adopt similar measures than those contemplated in the draft proposal, it is worth asking whether cloud service providers would be free to notify users (as contemplated in Recital 77 of the Draft proposal) in that country of any data access demands they had received from EU Member State authorities.

7. Interoperability (articles 28 to 30)

Article 28 sets forth essential requirements regarding interoperability. First, it is of paramount importance to define what is an operator of data spaces because these entities will be subject to these requirements. Platforms that serve to exchange data should not be subject to these requirements by default. For example, some platforms used today work very well to exchange data, and these platforms are not Blockchain enabled as required by 28.1(d). However, these requirements make sense for Common European Data Spaces. We would therefore suggest amending Article 28.1 to read that "*Operators of European Common data spaces shall comply with, the following essential requirements to facilitate interoperability of data, data sharing mechanisms and services."*

Second, Article 30 sets forth essential requirements regarding smart contracts for data sharing. The essential requirements of Article 30.1(b) and (c), as they relate to termination and interruption of smart contracts, data archiving and continuity, would best be applied to smart contracts that allow the exchange of value of assets, such as cryptocurrencies. This is because the requirements on termination and interruption aim to address issues and disputes that could financially harm one Blockchain participant over another. Archiving data for purposes of continuity will serve auditability and dispute resolution purposes, which again are useful in the framework of exchanging value or assets and are not required for other types of smart contracts, such as those deployed in member-only Blockchain enabled platforms.

Lastly, we fully agree that the access controls mechanisms referred to in Article 30.1(d) should be implemented. However, the level of implementation will depend on the type of smart contract and hence the relevant access controls needed for that specific smart contract (i.e., Blockchain application). For example, in the case of a permissioned Blockchain that only the members of such application are entitled to enter, access control is inherently imposed. But if the purpose and use of the Blockchain is to share with a wide audience, access control may not be required. The requirement that "access control must be protected at the smart contract layer" is also problematic if there is broader access control implementation.

* * * * *

BSA and its members support industry-led and other voluntary efforts to facilitate the use and sharing of data. We encourage the Commission, the Parliament and the Council to ensure that the Data Act supports such efforts and protects the rights of EU data owners to retain full control over whether they share or transfer data, to whom, and on what terms.

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315