BSA | The Software Alliance's submission to the EU Commission's Public Consultation On The EU Data Act

September 3, 2021

BSA | The Software Alliance ("BSA")[1] welcomes the opportunity to provide input to the European Commission's public consultation on the Data act and Amended Rules on the Legal Protection of Databases ("the Act"). BSA's members 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 is vital to the trust that customers place in BSA member companies and their offerings.

BSA supports efforts by governments to facilitate the sharing of data, and we welcome the Commission's focus on "*creat[ing] a fair data economy by ensuring access to and use of data, including in business-to-business and business-to-government situations*". The ability to share data both within the EU and across borders is critical to almost every organization in Europe and abroad. EU organizations of every size and in every sector rely on cross-border data transfers to source parts, support overseas employees,

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

Avenue des Arts 44
1040 Brussels
Belgium

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

collaborate with partners, and reach new markets and serve new customers. According to the Global Data Alliance, cross-border data transfers already contribute over two trillion Euros to global GDP, a figure that is sure to grow in the years ahead.[2] To ensure that EU companies can realize the full benefits of data, we support efforts by the EU Commission to remove regulatory impediments to data sharing and transfers, both within the EU and internationally, and to support mechanisms that promote voluntary data sharing between organizations.

In this submission, we focus on several sections of the public consultation and in particular: (1) Business-to-government data sharing for the public interest; (2) Business-to-business data sharing; (3) Tools for data sharing: smart contracts; (4) Improving portability for business users of cloud services; (5) Intellectual Property Rights – Protection of Databases; and (6) Safeguards for non-personal data in international context.

A general comment is 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 EU to share the data they own—or restricting them from sharing or transferring data, including across borders—will prevent EU organizations from reaping the full benefits of data and will render them less able to innovate or to compete effectively in global markets.

***

I. Business-to-government data sharing

The public consultation asks whether the EU should "*take additional action so that public sector bodies can access and re-use private sector data, when this data is needed for them to carry out their tasks in the public interest purpose*" (question 2), notably asking whether EU or Member-States' actions are needed in the matter. Contrary to the Inception Impact Assessment (IIA) which sets out options suggesting that access to such data would occur only with the consent of the private-sector entity holding the data (e.g., proposals to "facilitate agreement" on data sharing), the issue of consent in itself is not addressed in the consultation except indirectly via the questions pertaining to "incentives" (financial or non-financial) to that entity (questions 5,7 and 8).

BSA position and recommendation(s). BSA recognizes the value that societies can realize when private- and public-sector entities share data with one another. Indeed, for more than a year, in line with the public consultation's preliminary statement that "*the*

[2] *See* Global Data Alliance, *Cross-Border Data Transfers Facts and Figures* (2020), https://www.globaldataalliance.org/downloads/gdafactsandfigures.pdf.

COVID-19 crisis has shown the essential role of data use for crisis management and prevention", 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. But we are concerned that imposing data-sharing mandates on private companies could lead to unintended consequences, such as encouraging companies to be less transparent about the data they hold, seeking to store their data beyond the reach of EU authorities, and being less willing to collaborate with governments on data access issues. Accordingly, we would encourage the Commission to refrain from introducing mandated data-sharing and focus, 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.

However, and if the Commission does propose a data-sharing mandate in the Data Act, we would encourage any such mandate to respect the following principles.

1. First, any such mandate should be directed at the entity that owns and controls the data. As noted earlier, BSA members often act as processors for the data that their customers own and control. They 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.
2. Second, any data-sharing mandates 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 public 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.
3. Third, where the concept of "opening up data for public interest purposes" is an important principle, and where rights are granted for public sector to access privately-held data, the "public interest" element must be carefully balanced against the costs and risks this may entail. What defines "public interest" should follow a context-specific approach.

II. Business-to-business data sharing

The EU Commission stresses, in its public consultation, that "the Data Strategy intends to promote business-to-business (B2B) data sharing which will benefit in particular start-ups and SMEs, putting emphasis on facilitating B2B voluntary data sharing based on contracts".

BSA position and recommendation(s). First of all, BSA welcomes the intention of the Commission to put *"emphasis on facilitating B2B voluntary data sharing (…)*". BSA favors a tailored approach to data sharing, based on the need and specificities of the system, on voluntary basis, respecting the freedom of trade both within the EU and on the international stage.

We would, however, recommend caution on three issues raised in the public consultation, notably (1) model contract terms for voluntary use in B2B data sharing contracts; (2) horizontal access modalities regulating in a harmonized way how data access rights should be exercised; and (3) the "fairness test".

1. With regards the definition of a set model contract terms to be developed by the EU Commission, we would advise to rely on best practices, developed and used by the industry, which appear, in the matter, the best equipped to identify, develop and propose such best practices, to be applied on a voluntary basis. Such systems already exist and function well, with limited to none of the negative effects often faced by the weakest party. The Linux Community Data License Agreement[3] and the Open Use Data Agreement[4] are good examples of industry efforts to create tools that will democratize the value of data by making it easier for all stakeholders to voluntarily share data in a manner that is predictable and trustworthy.
2. With regards the proposed "*horizontal access modalities […] regulat[ing] in a harmonized way how data access rights should be exercised*", BSA again recommends that the EU Commission moves away from a one-size-fits-all approach and contemplates a tailored approach, based on the specificities and particularities of the systems.
3. With regards the "fairness test", BSA cautions that the introduction of a broad concept of fairness will likely increase the risk of litigation. In particular, without a common understanding of fairness in contracts across the EU – a concept which does not exist in some Member States – courts and competent authorities will need to step in at the national level to define the test's scope and functioning. The introduction of such a test will benefit larger businesses and their larger business customers, which have the legal resources to litigate, to the detriment of smaller businesses and smaller business users. It will also lead, through differing interpretations, to the further fragmentation of the Digital Single Market.

[3] The Linux Foundation Projects, Community Data License Agreement, https://cdla.io/

[4] Microsoft, The Open Use of Data Agreement, https://github.com/microsoft/Open-Use-of-Data-Agreement

III. Tools for data sharing: smart contracts

Through the public consultation, the EU Commission seeks to understand whether smart contracts could be an effective tool to facilitate data portability and data sharing, and notably to assess "the need of harmonized standards for smart contracts in order to ensure interoperability and what the essential elements of such standards should be".

BSA position and recommendation(s). Smart contracts are an ideal tool to record Internet of Things (IoT) device-generated relevant state information such as location, provenance or temperature for instance, and record such information onto a permissioned ledger. This will allow to capture an immutable record and ultimately provide a trusted transaction. Many areas in the industrial sector (e.g. logistics or supply chain management) can benefit from such trusted recordings, but also from integration and/or analysis of the data.

A legal challenge for scaling smart contracts lies in the need to avoid fragmentation and ensuring a harmonised approach to meet the requirements from the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market ('eIDAS Regulation'). Also, when it comes to standards for the interoperability and scaling of smart contracts, network interoperability and the concept of identity are key considerations. We believe several technical patterns (e.g. API based information exchange, event based information exchange, or cross network consensus) can help address these considerations and would recommend the EU Commission to further explore with the industry the essential requirements informing technical standards.

IV. Improving portability for business users of cloud services

The public consultation dedicates a whole section to "*improving portability for business users of cloud services*" where the EU Commission stresses it will "*evaluate whether self-regulation in the field of business-to-business (B2B) data portability achieved the desired outcomes or whether other policy options should be considered",* with questions 4 to 7 expressly contemplating EU legislative action in the matter. Moreover, the Commission stresses that outcome of the recent Summary Report on the public consultation on European Strategy for Data showed that 30.8% of the total respondents are of the opinion that the self-regulation is the appropriate best practice in area of data portability versus 22.6% stressing the contrary and 46.6% not expressing an opinion.

BSA position and recommendation(s). In principle, BSA broadly supports data portability. 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, some BSA members offer tools that their customers can use to facilitate the porting of

their data into and out of the service, in many cases using widely-used machine-readable formats if the customers wish to do so. Portability is also a right guaranteed by article 20 of the GDPR, which the public consultation tackles in its Section VI. In a B2B environment, where cloud providers do not have access to the customers' data, and therefore cannot, by themselves, differentiate between personal and non-personal data, portability is offered to business customers for all the data they have in the cloud provider's systems, irrespective of whether this is personal or non-personal.

Given that 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, BSA wonders whether there are any market failures to correct, beyond the "vendor lock-in" mentioned in the consultation, which the SWIPO Code of conduct is precisely designed to address according to the EU Commission[5], and therefore whether there is a real need for the Commission to impose legal mandates on this issue. Instead, we would encourage the Commission 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 at this stage already

Should the Data Act impose such portability mandates on cloud service providers, however, we would urge the Commission to take account of the following:

- *Create a level playing field & Refrain from imposing technology mandates.* Any portability obligation should also take into account that enterprise services are provided both from the cloud and on-premises. 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 (to be specified in implementing acts, as mentioned in the IIA) is a cause for concern as it will reduce choices for customers and impede innovation. To the extent the Commission imposes data or app portability mandates, it should focus on contractual restrictions that unreasonably prohibit customers from porting their own data. Any new requirements should be technology neutral, and apply equally regardless of the technology used.
- *Focus on customer access to tools.* Certain passages in the IIA (such as the text quoted above) could be read to suggest that cloud service providers should have an affirmative obligation to format customer data in certain ways, or to port that data to a different platform, and to "ensur[e] business continuity" in the process. This runs completely against the reality of the market as cloud providers typically have no visibility into their customers' business processes, or how they wish to reformat or otherwise handle their own data. Instead, any mandate on this issue should focus on ensuring that cloud service customers have access to tools that they can use to port

[5] *"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.

their own data and apps; requiring cloud providers to do this would be unworkable in practice.

V. Intellectual Property Rights – Protection of Databases

The public consultation mentions that "*the Commission published a report evaluating the Database Directive in 2018 […] conclude[ing] that the Directive could be revisited to facilitate data access and use in the broad context of the data economy and in coordination with the implementation of a broader data strategy*".

BSA position and recommendation(s). BSA strongly recommends that any review of the Database Directive and the Trade Secrets Directive should be done in a cautious manner so as to ensure that trade secrets, confidential business information or IP rights and protections are not undermined and run contrary to the objectives envisaged by the Data Act. Therefore, we urge the EU Commission to follow an evidence-based approach to identify whether any issues exist, before considering significant changes and to work with and within other international entities, such as the World Intellectual Property Organization (WIPO), who are also reviewing similar data issues, in order to have a harmonized system and prevent market fragmentation, difference in legislations globally and legal uncertainty.

VI. Safeguards for non-personal data in international context

The Commission lays out, in the last question of this section, different options to, "*at an EU regulatory level [`…] mitigate the risk for European companies stemming from the request for access by foreign jurisdiction authorities to their data*". These includes notably (1) "*Introducing an obligation for data processing service providers (e.g. cloud service providers) to notify the business user every time they receive a request for access to their data from foreign jurisdiction authorities, to the extent possible under the foreign law in question*"; (2) "*Introducing an obligation for data processing service providers to notify to the Commission, for publication on a dedicated EU Transparency Portal, all 42 extraterritorial foreign laws to which they are subject and which enable access to the data they store or process on behalf of their business users*"; (3) "*Introducing an obligation for data processing service providers to put in place specified legal, technical and organisational measures to prevent the transfer to or access of foreign authorities to the data they store or process on behalf of their business users, where such transfer or access would be in conflict with EU or national laws or applicable international agreements on exchange of data*".

BSA position and recommendation(s). BSA cautions against any restriction on the freedom of companies to transfer data across borders, as these transfers are an essential and necessary part of modern commerce 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*."[6] 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. The 'Global Data Alliance'[7], a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on data transfers has published several documents highlighting the need for such cross-border access to cloud-based technology and data in different sectors (e.g. innovation, supply chain management, remote health and remote work). Any restrictions on such transfers should therefore be limited to what is strictly necessary to serve a legitimate public interest, and be limited to the least trade-restrictive option available.

The cross-border data transfer restrictions proposed in the public consultation 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. In BSA's experience, it is exceedingly rare for data lawfully disclosed to third-country law enforcement authorities to end up being exploited commercially without the data owner's consent. And it is exceedingly unlikely that law enforcement demands for *non-personal* data will infringe upon fundamental rights set out in the Charter. 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.

Without a solid evidentiary basis for the necessity of such a restriction, and proof that the measure is the least-trade-restrictive means available, these restrictions might also be

---

[6] OECD, *Digital Economy Outlook*, ch. 1 (2020), https://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm.

[7] The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to innovate and create jobs. The Alliance supports policies that help instill trust in the digital economy while safeguarding the ability to transfer data across borders and refraining from imposing data localization requirements that restrict trade. Alliance members include BSA members and Abbot, American Express, Amgen, AT&T, Citi, Cortex, ExxonMobil, FedEx, General Motors, Lego, Lumen Technologies, Mastercard, Medtronic, NTT, Panasonic, Pfizer, RELX Group, Roche, United Airlines, Verizon, and Visa. BSA | The Software Alliance administers the Global Data Alliance.

inconsistent with the EU's trade commitments, as they could have a disproportionate impact on cloud service providers with foreign operations or otherwise engaging in cross-border trade. Given that any organization with foreign operations (not just cloud service providers) could be subject to data access demand from foreign authorities, it is also unclear why the Commission proposes to limit this restriction only to cloud service providers, and not to any organization that might be subject to an access request from third-country authorities.

We also urge the Commission to ensure that the proposed Data Act is fully consistent with the EU's broader commitment to free and fair trade. The Commission will undoubtedly wish to avoid proposing any measure that is inconsistent with this commitment. Indeed, if a third country were to adopt the measures contemplated in the public consultation, it is worth asking whether cloud service providers would be free to notify users in that country of any data access demands they had received from EU Member State authorities. We take it as a given that the Commission would wish to avoid imposing rules with regard to foreign authorities that authorities in the EU could not themselves comply with.

* * * * *

BSA and its members support industry-led and other voluntary efforts to facilitate the use and sharing of data. We encourage the Commission 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