IBM Submission to the European Commission on the Data Act Consultation

IBM welcomes the opportunity to contribute to the European Commission's consultation on the upcoming Data Act, and to offer our views on the measures we believe can help fostering data sharing while safeguarding the rights of data holders and avoiding undermining trust in technology.

B2G and B2B Data sharing

We agree with the European Commission that encouraging data sharing is an important element for the competitiveness of European businesses. Rules covering data access and usage rights should however not be intrusive or create onerous requirements. Contractual freedom and a voluntary approach should remain the foundation of data sharing policies which provide greater legal certainty and increased trust for businesses to share their data.

In B2G data sharing scenarios, we support the concept of "opening up data for public interest purposes" as an important principle. However, mandatory data sharing obligations should only occur where there is objective evidence that the public interest can be served and must be carefully balanced against the costs and risks these obligations may create. Against this background, the concept of "public interest" should be narrowly defined at European level to avoid fragmentation and follow a context-specific approach, as recommended by the High-Level Expert Group on Business-to-Government Data Sharing [1]. Broad and unspecific references to public interest without further definition are likely to discourage participation in the planned European data spaces, particularly by commercial entities. Any mandate to share data in the public interest should be accompanied by appropriate safeguards, such as strong purpose limitation requirements to avoid that the data is re-used for other objectives and retention periods aligned with the timeframe in which data remains relevant and up-to-date.

Also, any mandated data sharing regime should take into consideration the position of the data contributor under data privacy laws and differentiate obligations of a processor versus a controller. Data sharing obligations imposed on processors, who do not have control over their customers' data, could lead to a breach of processors' contract commitments or even conflict with EU or Member State legal requirements, thereby leading to legal uncertainty for both processors and controllers, and ultimately undermining trust in technology.

Compensation schemes based on marginal costs for dissemination and fair return on investment remain the fairest basis, although this may vary depending on the specific area of public interest. We encourage the European Commission to continue the dialogue with stakeholders and to conduct an assessment to put in place adequate compensation schemes for B2G data sharing, should it ultimately be necessary to implement.

In our view, the better way to increase data sharing is by promoting existing practices and tools such as Open Data Agreements; for instance the Community Data License Agreements[2], a cross-sectoral data license agreement available for widespread use. Standardised data sharing agreements can facilitate collaborative approaches for sharing data resources and have the potential to dramatically reduce transaction costs and licensing uncertainty. In

[1] Alemanno, Alberto, Towards a European Strategy on Business-To-Government Data Sharing for the Public Interest (October 16, 2020). Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing European Commission, 2020, HEC Paris Research Paper No. LAW-2020-1394, Available at SSRN: https://ssrn.com/abstract=3713320

[2] https://cdla.dev/

particular, some agreements implement the necessary arrangements to ensure that downstream recipients of data can freely use, modify or analyse data.
B2B contractual fairness test should be drafted with input from relevant stakeholders. We recommend that the Commission considers precedents and best practices that draw from experience and working methods established in other communities, such as the open-source community. Community-led efforts in drafting and gathering feedback (e.g. via the Linux Foundation, Apache Foundation and Eclipse Foundation) and central administration of the licenses by the Open Source Initiative have now resulted in a set of tried and trusted licenses that are widely used.

Furthermore, we agree with the Commission that horizontal modalities for access to data should be looked at further to iron out any potential contradictions between existing laws and regulations with the EU's objectives on increasing data sharing in a secure and trusted manner. However, horizontal rules on mandatory data sharing should be avoided, as this could discourage stakeholder participation in the Data Spaces, and in general, we caution against implementing various standards across different sectors. Certain types of applications will require a holistic view of various domains and will hence necessitate data from several sectors – for instance a system used for eco-friendly improvement of food chain supplies may require data related to agriculture, weather, fisheries, mobility, and retail. Successful commercialization of these type of applications relies on interoperability of such data and fair rules in obtaining access to such data.

We recommend that the EU forms a representative community to support, create, and promote mechanisms for making data available, by having all the right stakeholders, including from the technical community, around the table. We believe that issues that may arise in certain concepts can be ironed out through community driven efforts and feedback in order to help identify issues and more importantly, implement solutions. In our view, developing model contract terms centrally with stakeholders, for instance, by establishing a task force to help identify relevant checks and balances, whilst also drawing from decades of experiences based on other community working methods, could be an effective way forward for the purposes of achieving the contractual objectives of the Data Act. A similar approach to laying down data access and usage rights for non-personal data could contribute to sound policy-making.

Smart contracts

Smart contracts are an ideal tool to record real-time information generated by IoT devices onto a secured ledger. This allows the capture of immutable records, and thereby ultimately provides trusted transactions. Therefore, these contracts can also be very effective to technically implement data sharing. This however entails several considerations.

First and foremost, legal challenges need to be addressed, such as harmonization, for instance when it comes to the requirements from the eIDAS Regulation. The intersection of smart contracts and GDPR needs to be considered and the benefit of blockchain technology should be leveraged to support the goals of GDPR, in various ways, as outlined in our Whitepaper[3]. For example, while blockchain and GDPR started with very different goals—creating a currency independent of a central authority versus introducing data privacy laws—the two initiatives are aligned on the principles of secured and self-sovereign data (individuals in charge of their data).

Second, key technical conditions are needed to enable scalability of these contracts. Network interoperability is one of them. For instance, all parties must be able to identify and authenticate members from other networks. Self-sovereign identity and Decentralized identifiers ("DIDs") can help solve identity issues by establishing the trusted identity of a participant across networks without reliance on a centralized authority. Another important technical challenge for data sharing is the mutual understanding of the semantics of the data, as networks can use the same terms with different meanings.
To solve these technical considerations, we recommend that the European Commission fosters the adoption of

[3] https://iapp.org/resources/article/blockchain-and-gdpr/

industry-wide standards, as we believe that several technical patterns (such as API- or event-based information exchange for network interoperability, or self-sovereign identity) can help address interoperability concerns. We stand ready to engage with the EU Commission to further explore the essential requirements informing technical standards.

Data portability

We believe that self-regulation in the field of business-to-business (B2B) data portability achieves the intended outcomes of Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union. Therefore, other policy options are not necessary. The requirements of the Codes of Conducts should be reflected in contractual arrangements between cloud services provider and cloud customers to be effective, not in legislative instruments. Legislative action may be premature in this area, given the many ongoing industry-led efforts, notably industry code of conducts (SWIPO) and standardisation (ISO 19441). Policymakers should support industry-driven efforts on guaranteeing portability for the purposes of creating market awareness and generating more trust in the cloud market.

Review of the Database and Trade Secrets Directives

We support the development of frameworks that encourage more data access and data use, while protecting intellectual property (IP) rights and commercially-sensitive information. Any review of the Database Directive and the Trade Secrets Directive should not undermine trade secrets, confidential business information, or IP rights and protections and 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. We also urge the European Commission to stay connected with other international entities, such as the World Intellectual Property Organization (WIPO), who are also reviewing similar data issues.

Government access to data

As an enterprise Cloud Services Provider, IBM has a longstanding commitment to protecting client data[4] and we support the European Commission's ongoing international efforts to facilitate free flows of data based on a foundation of strong data protection and security. International data flows are indispensable for European companies' competitiveness and the Data Act should strive to remove - and not institute - conflicts of laws, and be fully consistent with the e-Evidence regulation and other EU legal constructs (such as the Data Governance Act's introduction of GDPR-like adequacy decisions on third-country IP and trade secret regimes), as well as the EU's international commitments for instance under the WTO agreements.

We believe that any concerns about foreign government access to data should be addressed through multilateral governmental negotiations establishing common baseline expectations. This is more efficient, more effective and more stable than a design where each government creates its own regime, shifting the burden to individual companies to try to comply with the varied, and potentially, conflicting requirements of governments worldwide. In view thereof, we call on governments to develop a global consensus on a durable, multilateral approach among like-minded international partners to ensure adequate safeguards for government access to data.

If such consensus cannot be reached with certain countries, we recommend that before contemplating new regulatory intervention, the European Commission considers developing and fostering the adoption of voluntary and future-proof guidelines/best practices that service providers can implement, and companies can require as a matter of contract. Protecting a company from misuse of their non personal data is different from protecting an individual from misuse of their personal data, and the solution should reflect that. Companies are in the best position

[4] https://www.ibm.com/blogs/think/2014/03/open-letter-data/

to determine how to protect against the misuse of their non-personal data, based on the nature and sensitivity of their data, the technical and organizational measures provided by the selected Cloud Service Provider and such Provider's data handling practices. Protecting a company's non-personal data can best be accomplished through the establishment and adoption of best practices for lawful access to non-personal data, rather than through overreaching regulation of business. In order to establish effective best practices, it would be beneficial for all stakeholders if the Commission could share relevant non-identifying examples of where a government has been found to have used government process to access non-personal data for commercial purposes.

For instance, US surveillance laws and implementing regulations limit the purposes for which data can be collected, and commercial usage is not an authorized purpose. US law enforcement and government requests for information generally seek to establish facts and circumstances about criminal activities of individuals. Companies' commercial data typically are not the subject of these requests. Consequently, the idea that commercial data would be included under lawfully requested information and exploited commercially without the data owner's consent is highly questionable. We also wonder to what extent such demands for non-personal data could infringe upon fundamental rights set out in the Charter. For these reasons we recommend that policy options carefully consider the difference in risks and dimensions between personal data and non-personal data when it comes to addressing lawful disclosure to third-country law enforcement.

Furthermore, the concept of data needs to be evaluated in this respect. For instance, should the same safeguards apply to customer contact data or to metadata generated through the provision of the cloud services than to data entrusted by a customer to the provider of its choice?

Also, it is important to tailor policies on government access to data to Cloud Services Providers' business models and data handling practices. Not all Cloud Services Providers are the same[5]. For instance, enterprise business models support businesses and organizations, and involve business data, which generally is not the target of third country authorities' requests, because it provides little use for national security intelligence purposes. Digital consumer platform business models, on the other hand, involve direct interaction with consumers and collect and control vast amounts of consumer data. This differentiation is key as government access to data requests generally involve efforts to combat serious crime, including terrorism, and usually target electronic data held by consumer digital services companies and platforms that may contain evidence of a serious crime.

To fully meet its purpose, any contemplated transparency requirement (such as an obligation to report all the foreign laws with extraterritorial effect) should apply to all CSPs active in the EU regardless of the origin of their headquarters and take into account the actors involved in cloud delivery models. As a principle, transparency policies should ensure a level-playing field, be proportionate to the risks and non-discriminatory, but also be relevant and tailored to the risk. It is not useful for cloud customers, users or the general public to obtain a long list of laws with extraterritorial effect to which all entities of a multinational group are subject, including Tax laws or Non-Bribery regulations. Therefore, transparency obligations should be carefully crafted to avoid any unnecessary burden that would result in confusing the reader, and therefore miss their purpose.

We support policies that require CSPs to notify their clients (who can then turn to their users) in the case foreign authorities seek content data pertaining to these clients, to the extent permitted by the applicable foreign legal framework. This is and has been a long-held practice at IBM.

[5] https://www.ibm.com/policy/government-access-to-data/