Japan Business Council in Europe

13th of May 2022

Initial Views on the Data Act Proposal

The Japan Business Council in Europe (JBCE) would like to welcome the Data Act proposed by the European Commission to promote fairness in the use of and access to data. We believe that the use of data among various stakeholders is essential to strengthen the competitiveness of companies and to create a fair society where everyone has the opportunity to innovate.

However, we are concerned that certain types of requirements within the Data Act are too prescriptive and could therefore represent a risk to innovation, rather than an opportunity to help drive it. Additionally, we would like to draw attention to the fact that the Data Act overlaps with many other pieces of legislations – such as on the issue of data portability which is covered in the GDPR but also in other texts. We therefore believe that the Act should be amended with this in mind.

We would like the new legislation to strike a balance between rights to access data and incentives to invest in data, with a simple and workable framework for all stakeholders.

In this document, JBCE would like to express its initial views on the Data Act. We will continue to contribute to the discussion on this legislative proposal in a constructive manner by providing our suggested amendments later on.

Below is a summary of our initial views:

Definition and Scope (Article 1-2)

- JBCE believes that it is appropriate to promote sharing and use of data in general.
- The subject and scope of the Data Act and some of the definitions could be further clarified.

Balance of rights between B2C/B2B in data sharing (Article 3-12)

- Paying full respect to development efforts and trade secrets is essential so as to consider the obligations of data holders.
- It would be an excessive burden to design and manufacture all products and related services in order to make data easily and directly accessible to the user by default.
- The new data portability right should be aligned with the personal data portability right envisaged in the GDPR.
- Provisions on unauthorised use or disclosure of data need to be reconsidered, taking into account that once disseminated, data is difficult to completely destroy.

Balance between public interest and protecting business confidentiality (Article 14-22)

- Clarification should be provided to narrow “an exceptional need" for the provision of data.

Switching between data processing services (Article 24)

- The language on the “full continuity” of services should be aligned with other Articles which place the emphasis on “functional equivalence” instead.

International data transfer and standardization (Article 27-30)

- International data transfers should be carefully considered in accordance with international standards.

Japan Business Council in Europe

Governance and application (Article 31-42)

- Penalties should be well-balanced so as not to discourage business, investment and innovation.
- Due to complexity and severity of the requirements, an application time of 12 months after the entry into force would be better to be extended to 36 months.

1. Definition and Scope

(1) Article 1 & 2

While we acknowledge it is hard to set ownership rights for data, we welcome the intention of the Data Act to broaden the use of non-personal data. However, based on the understanding that business is conducted in a context wherein the right to use data generated by IoT devices doesn't currently exist, we believe that the Data Act should be introduced with caution. This is indeed the introduction of a new way of thinking about data usage for business and should therefore clearly exclude contracts (sales and provision of services) which were made prior to the enforcement of the Data Act. Retroactively addressing data and contracts prior to the enforcement would place undue burdens on businesses.

(2) Recital 14 & Article 2 (1), Article 3(1), Article 5(1), Article 6 (2)(c)

In our view, the definition of data is too broad which results in compliance issues for businesses. It is difficult for businesses to comply with the Data Act's provisions to further promote data sharing since the Data Act encompasses both personal/non-personal and raw/inferred data. JBCE fears that such a combination would potentially would lead to an endless expansion of the scope and believes that the definition of data should be refined.

We suggest that Chapters II-IV on B2C and B2B data sharing should apply only to non-personal data. Under Article 3(1), manufacturers are obliged to design and manufacture their products in such a way that the data generated by their use is easily and securely accessible to the user. However, allowing users to directly access all data generated by the use of the product could pose serious concerns for the security of any personal data generated.

Additionally, Article 2 (1) includes photographs and movies as data, but because they can be copyrighted and related to creative works, it should be clarified that only the photographs and movies generated by the products are within the scope.

More explanations should also clarify Recital 14 and Article 6 (2)(c) regarding what 'information derived or (is) inferred from this data' and 'the data available it receives to another third party, in raw, aggregated or derived form', respectively.

Furthermore, it is not practical to handle such data in some cases, because the data is often edge-processed within products or related services as soon as it is collected, and there is no raw data which can be shared. In these instances, raw data is immediately deleted once it is processed due to the fact that its volume is too large to store.

Moreover, it would not be feasible to send data continuously and in real-time due to its volume. Therefore, the definition of "continuously and in real-time" makes it difficult to assess in which interval this would be accepted.

In this sense, workable rules based on technical feasibilities and business practices would be needed.

Finally, the new data portability right envisaged in Article 5(1) of the Data Act should be aligned with the personal data portability right envisaged in the GDPR. More specifically, Article 20(2) of the GDPR states that the data subject has the right to have their personal data transmitted directly from one controller to another, where technically feasible. The same caveat should be added to Article 5(1) of the Data Act wherein the data holder must, upon request from the user, make available to a third party the data generated by the use of a product or related service only if such a process is technically feasible.

(3) Article 2(2), Recital 15

Recital 15 excludes devices which are primarily designed to display or play content, or to record and transmit content from the scope of products covered by the Data Act. However, the definition of 'product' in Article 2(2) is not consistent with Recital 15. Article 2(2) states that products whose primary function is not the storing and processing of data are included in the Data Act's scope. We believe that, to ensure clarity, Article 2(2) should mirror Recital 15 and explicitly state that products primarily designed to display or play content, or to record and transmit content are excluded from scope. Furthermore, even though printers or TVs are notably devices, primarily designed to display or play content, they are not explicitly mentioned in the list of examples of such devices that Recital 15 provides. To ensure clarity, we recommend that printers and TVs should be added to this list.

(4) Article 2(5)

The Commission's proposal does not make any difference between users, while there is a variety of situations that would require a more granular approach.

Users can be private customers, but also companies owning connected products that they further lease or rent to other users. In this situation, the end-user is entitled to accessing data, but the data holder is not in a position to grant and manage this right to access.

The Data Act should make clear that it is the company in touch with the end-user that must be in charge of managing the permission of the end-user to access data.

Subsequently, the obligation of the data holder should be limited to a 'primary user' that rents or leases a product or receives a service from the data holder itself. Article 2 should be amended accordingly, to offer legal certainty.

In an economy where consumers increasingly purchase services rather than physical products, the situation for data holders described above is likely to become increasingly commonplace, thus reinforcing the need to provide clarity on this point.

(5) Article 2(12)

The definition of the provider of data processing service would need to be clarified. We recognize that IaaS, PaaS and SaaS are in the scope, and that should be clearly stated. We believe that, for example, data analysis and data transaction services should be out of scope, when their cloud infrastructure is provided by another data processing services provider. It should be also clearly stated.

2. Balance of obligations among related parties

(1) Article 3(1)

It would be an excessive burden for companies to design and manufacture all products and related services in order to make data easily and directly accessible to the user 'by default'.

Products and related services are currently designed to collect and transmit only a fraction of all the data that is being generated to allow their proper functioning. Without a clearer definition of 'data', the Act suggests that absolutely all data would have to be provided to the user. This would include data that the provider of the device itself cannot access for the moment, and would therefore imply major design changes, exponential increase in computing power and in the volume of data transferred. The cost incurred would not be compensated, as this additional data would be of little interest to the user or to third parties.

The collection methods, as well as the collected data, are inherently trade secrets which we should not be forced to disclose. A clarified definition or limitation of 'data' would decrease this burden.

Article 3 mentions that data should be "directly" accessible. There is no definition for this concept added to the current draft Data Act, as such, providers of connected devices cannot determine what is expected in order to meet this requirement. Recital 21 provides a useful clarification, by reading that 'Products may be designed to make certain data directly available from an on-device data storage or from a remote server to which the data are communicated'. A similar provision should be included in the Regulation text itself, so as to provide legal certainty for providers of connected devices.

Finally, the Commission's Proposal stresses cybersecurity as a requirement for the provision of data to the user and the third party. We strongly support this principle and insist that manufacturers of connected devices are free to decide the most appropriate technical and organisational solutions to meet their obligation in this respect.

In addition, we suggest adding the concept of 'safety' to the list of requirements for providing access to data. Depending on the connected device considered (e.g., a vehicle, an industrial machine…) access to data should happen in a way and at a time that does not interfere with the normal operation of the product. Like cybersecurity, the manufacturer of the device should be free to determine the most appropriate solution to ensure the safety of the product and of its users.

(2) Article 4(1) & 4(6)

Companies develop products with an intention to make full use of the data generated by the use of the products and services for future developments and so forth. Therefore, although we welcome the intention of the European Commission to increase data usage and give single market participants countless opportunities, we think that the value of data that data holders, or in this case, manufactures generate, would need to be fairly evaluated. We would like to argue that clearer incentives would be needed for data holders or manufacturers and that making data available 'free of charge' should be excluded in commercial applications. Moreover, data holders or manufacturers should be able to use the data as the users do to maintain a level playing field for all single market participants as much as possible.

Otherwise, data holders or manufacturers would hesitate to further invest into developments, which would stifle innovation.

In this regard, voluntary agreements rather than a mandatory approach for B2B data sharing would be preferable.

(3) Article 4(3) & 5(8)

As far as we understand, only a raw data is under the scope of the Data Act, but it is unclear how to make such data available when it comes to connected devices while fully respecting trade secrets and intellectual property. For example, a careful consideration of data generated by connected devices is required, as it often comes in unreadable formats (e.g., zero and ones etc.). To make it readable, a certain level of knowledge is needed on the part of the manufacture of the device. In turn, this begs the question of how to distinguish between the rights of the user and the third party to access this 'readable' data. It further presents the challenge of balancing the rights between a data holder and user/third party and to avoid creating a favourable environment for one side and while undermining the other.

Articles 4(3) and 5(8) address the protection of Trade Secrets, when data is shared respectively with the user and third parties.

In both cases, the data holders can rely on "specific necessary measures" agreed with the user or the third-party receiving data. However, there is no definition of what these measures can be and how they can be enforced.

Article 5(8) also mentions that trade secrets should be shared if "strictly necessary" to fulfil such a purpose agreed between the user and the third party. However, it is not clear who is in charge of determining this aspect. We consider that the trade secret holder should be the one in charge of deciding what trade secrets should be disclosed.

(4) Article 8(3) & 9(2)

We see in these articles that 'fair, reasonable and non-discriminatory' (FRAND) obligations are to be implemented. However, these obligations are for licensing patents which are essential for conforming to a standard in the first place. Based on this understanding, we do not believe that FRAND obligations, or their equivalent, should be imposed on data transactions. Data handling that inhibits competition should be regulated by the competition law which would be more appropriate to contribute to establishing a fair single market where the utilization of data is accelerated.

We would like to reiterate that commercial incentives are needed from the point of view of businesses. In addition, the data used among partner enterprises and linked enterprises should be out of scope.

(5) Article 8(4)

This article says that 'A data holder shall not make data available to a data recipient on an exclusive basis unless requested by the user under Chapter II', but an exclusive contract should be possible if there is a risk to intellectual property rights or trade secrets.

3. <u>Disposal of data</u>

(1) Recital 33, Article 6(1) & 11(2)

These articles stipulate that data made available to a third party or a data recipient should be deleted when the data are no longer necessary for a third party or data are disclosed in an unauthorised way. However, practically speaking, it would not be realistic to ensure the effectiveness of these Articles given that it is virtually impossible to erase those data and because the moment the data are shared, they are instantly utilized in various ways.

Third parties use data received from users to deliver the service requested, but could also use them for other purposes, e.g.: train new algorithms (R&D&I) internal to the recipient company or, once anonymized, to another partner company (in the case of start-ups for instance), aggregated/processed for statistical or other uses too (e.g., information on traffic flows to municipalities, etc). As the current draft mandates the deletion of the data (Article 6) or its use only for the service agreed with the user (Recital 33), certain services, already on the market today, could be at risk and the Data act would prove to be a blow to innovation rather than a boost.

In addition, especially regarding Article 11(2), a clarification of the exemptions would be needed. The criteria for “significant harm to the data holder” and “disproportionate in light of the interests of the data holder” are unclear and difficult to determine.

4. Exceptional needs

(1) Article 15

Clarification should be provided to narrow down “an exceptional need" and "public emergency." Article 15 (c) states that ‘where the lack of available data prevents the public sector body or Union institution, agency or body from fulfilling a specific task in the public interest that has been explicitly provided by law…’. In our view, if it is not a "public emergency," there must be no urgency to impose an obligation to provide data. In such instances, public entities should enter into an individual contract with the data holder to receive the data.

Therefore, we think that the European Commission should clarify, through the creation of a clear and comprehensive list or through guidance, "exceptional needs (exigencies)" harmonized at the EU Member State level. If a mandatory scheme were to be introduced, it would certainly be the public authorities who would decide when a request for data sharing based on "exceptional needs" would arise, and such unilateral decisions could create legal uncertainty for companies. We are also concerned with the lack of clarity regarding the reasons provided for the exclusion of SMEs when exceptional needs arise.

(2) Article 21(1)

We would like to underline the importance of the clarification of “exceptional needs”. In this Article, it can be read that even in the absence of an emergency response, company data can be passed on to various research institutions. However, reasonable compensation should be paid to the data holders.

5. Switching between data processing services

(1) Article 24(1)(a)(2)

According to this this article, data processing service providers are obliged to include in their contracts clauses which guarantee ‘full continuity in the provision of the respective functions or services’ during the transition period of transferring a customer’s data to another provider. However, in reality different service providers often provide different sets of services which

sometimes have different specifications. Due to this, it would not always be possible for the provider to ensure 'full continuity' during the transition period. We suggest that the term 'full continuity' should be replaced with the term 'functional equivalence', which is already used in articles 23, 26 and 27.

6. International data transfers

(1) Article 27(1) & (3)

Since the provision of Article 27(1) appears to regulate the transborder transfers of non-personal data in general, the text should clarify that the provision is intended to prevent unrestricted data transfers in response to data transfer requests not based on international agreements from third country law enforcement agencies and others. Additionally, we are concerned that the detail of 'all reasonable technical, legal, and organizational measures' is not provided in the Act and that the guidelines will be developed separately.

With regard to concerns about access to data by third-country governments (government access), we believe that rather than placing an obligation on data processing service providers, such as cloud, edge, etc., we should consider addressing it in accordance with international standards and rules at multilateral government consultations, such as the OECD.

7. Penalties

(1) Article 33(1)

If penalties are to be different in Member States, we believe that transparency will be low. Therefore, if penalties are to be established, they should be clearly defined.

Penalties themselves raise fundamental questions as they may inhibit the use of data. If penalties are to be introduced, they should be well-balanced so as not to discourage business activities.

8. Application

(1) Article 42

The Commission's proposal only provides a 12-month lead time for an organisation to comply with the requirements of the Data Act after its entry into force.

Given the complexity and severity of some of the requirements particularly for connected products as well as on the business model of companies that are marketing these products and related services, we would recommend that the Data Act apply 36 months after its entry into force.