10 May 2022

JEITA Comments on the Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)

The Japan Electronics and Information Technology Industries Association (JEITA) is Japan's leading digital association, with around 400 members from Japan and abroad. We are working not just with the digital sector but all sectors to realize "Society 5.0" as a society in which data drives innovation and innovation drives social advance.

JEITA welcomes this opportunity to comment on the EU's proposed Data Act. We would appreciate the following comments being reflected in the final legislation.

1. General comments

JEITA supports the European Council's objectives and directionality in seeking to develop a common EU framework that facilitates access to and the sharing and use of data and opens the way for data-led innovation.

However, in relation to access to and sharing of company-held data, we believe that from the perspective of protecting intellectual property rights and company secrets, as well as to avoid disadvantaging end users by discouraging companies from investing in data-related business and causing them to hold off from business development, rather than taking a compulsory approach, the approach should instead be to have companies make discretionary contracts on their own accord so as to secure business freedom and foster innovation, thereby encouraging incentive-based data sharing.

2. Specific points

(1) Article 2: Definitions

- The definition of "data" as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording" is so broad that it could include photograph and film copyrights, as well as related creations. These should be explicitly noted as outside the scope of the Data Act. In addition, given that is technologically impossible to transfer specific data reliant on software components and components in connected products such as IoT devices to other devices, such data too should be explicitly excluded.

- Point 15 in the preamble notes that "certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation." As it is unclear solely from the "product" definition in Article 2.2 that such products are excluded from the scope of the Data Act, the language from Point 15 should be added to the "product" definition in Article 2.2. In addition, the particular products noted in Point 15 are "personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners"; please add televisions, which are clearly also "products that are primarily designed to display or play content," to this list of examples. As Point 15 further notes that products that require human input should not be covered by the Regulation, we request that you also add to the list of

examples projectors, multifunctional photocopiers, and printers that are used for multiple purposes in offices, etc.

- Please exclude data that has been destroyed by data-holders. When large volumes of data are acquired, because of the practical difficulty of storing and providing all that data, the usual practice where data is acquired at the edge is to process it there immediately, deleting unnecessary data. In addition, when large amounts of raw data and processed data in a state inseparable from said raw data are generated and deleted, it is not practical to supply "all" raw data after extracting the processed data excluded from the scope of the Regulation because this contains intellectual property rights. Neither is real-time data transmission practical, as large data volumes put pressure on communication lines. We ask that you seek the views of industry so as to create appropriate rules aligned with business realities.

- In terms of the data and contracts covered under the Data Act, please clarify that data created and/or acquired and contracts signed before the Act enters into force shall be exempt from the Act. Retroactive application of the Data Act to data and contracts pre-dating enforcement would impose an excessive burden on companies.

(2) Article 3: Obligation to make data generated by the use of products or related services accessible

- Article 3.1 notes that providers of products and related services must design those products and services in such a manner that data generated by their use are, by default, easily, securely and, where relevant and appropriate, directly accessible to the user (consumers and user companies). Giving users direct access to device logs and other data that does not contain personal information, however, would cause major security concerns. To ensure product security, the non-personal data addressed by the Data Act should be narrowly defined based on a detailed analysis of security risks. Safety in terms of security should also be considered as a condition for users being able to directly access data.

- It is unclear what it meant by "directly accessible" in Article 3.1. For example, does it mean that users should be able to acquire data immediately upon accessing websites and connected products? Would disclosing data upon receiving a disclosure demand from a user also be deemed as direct access to data? Various methods of data access should be allowed, and in addition to clarifying what is meant by "directly," disclosing data upon receiving a disclosure request from a user should also be deemed direct access.

- Data generated by or used in connected products presupposes the use of data from multiple products and necessarily entails connection to other companies' products. In such cases, however, it would surely be extremely difficult to identify which data was generated or being used in which product. Accordingly, the concern would be that users too would be unclear as to which service provider they should approach to get the data they seek.

- Article 3.2 requires that certain information be provided to the user "in a clear and comprehensible format," including "(a) the nature and volume of the data likely to be generated by the use of the product or related service" and "(b) whether the data is likely to be generated continuously and in real-time." In both these cases, putting together and providing that information prior to the conclusion of a contract would be difficult and would also run the risk of different handling after the start of use.

What data is used and how and when it is acquired in what part of a device are company secrets. Forcing all companies to disclose company secrets is simply out of the question, and compulsory disclosure should be limited to data which the user has intentionally recorded. Further, given the extent of the burden imposed on the data holder, it would be unacceptable for the obligations imposed by Article 3.2 to be applied in perpetuity or for data to be provided free of charge to the user.

(3) Article 4: The right of users to access and use data generated by the use of products or related services

- Article 4 requires that where data "cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time," in which case the cost of providing that information in real-time should be calculated and a charge at least levied on the user.

- Requiring companies to garner the consent of product users from an equal position so as to protect company secrets would impose a major burden on companies. Company secrets comprise a company's information assets and should be distinguished from data acquired from users.

(4) Article 5: Right to share data with third parties

This article requires that upon request by a user, the data holder must make available the data to a third party without undue delay, continuously, and in real-time. That data includes both personal data and non-personal data. While this is an excellent move in terms of recognizing the right of the user to data portability, in reality, it may be a technically impossible requirement for data holders. Given that the GDPR limits the right to data portability to cases in which this is "technically feasible," the Data Act is more restrictive by comparison. It would be appropriate to add the condition of technical feasibility to the Data Act as well.

(5) Chapter III: Obligations for data holders legally obliged to make data available

- We support the European Council's objectives and directionality in seeking to facilitate access to and sharing of data generated by connected products and related services and encourage EU innovation.

However, promoting data-sharing among companies also creates risk around the disclosure of intellectual property rights and company secrets. We therefore believe that rather than a compulsory approach, it would be better to proceed on the basis of discretionary contracts voluntarily formed between companies. The non-binding model contract provisions to be drafted by the European Council would also be useful in this regard. Moreover, given industry best practices, support and incentives should be provided so that companies voluntarily share data.

- Data transactions within the same corporate group should not be treated as equivalent to data transactions with third parties. Because companies within a corporate group often work together on a business line, applying Data Act obligations in relation to transactions among

companies, and particularly FRAND obligations, even to transactions within the same corporate group would cause major business concerns. Where data is given to a group company, data sharing with other companies belonging to the same category should not be made a non-discriminatory condition.

- While the proposed Data Act and other proposals related to the European Council's legislative framework for promoting data sharing among companies comprise one of the core objectives of the European Data Strategy announced in February 2020, from the perspective of EU antitrust legislation, the exchange of information important in terms of competition, and particularly exchange among other rival companies, could comprise a grave antitrust violation.

To promote data use and ensure legal certainty, measures should be investigated to enable data sharing with other companies without antitrust legislation being applied pursuant to the Data Act to companies holding data generated from the use of products and related services.

(6) Article 6: Obligations of third parties receiving data at the request of the user

- At the point when data is no longer needed, while it can probably be deleted from the company's own products, this is far more difficult in the case of other company's connected products.

- It is impossible to distinguish the difference between improving the performance of a company's products and developing a product for the purpose of competing with rival companies. Because this provision would also prevent the use of data for improving the performance of a company's products, it could block companies from developing products and upgrading performance based on data analysis.

(7) Article 8: Conditions under which data holders make data available to data recipients

- Under this provision, where a data holder makes data available for the use of data recipients, the data holder is required to demonstrate that there has been no discrimination among the various recipients. However, because the requirements of a non-discriminatory situation are not clear, it would be difficult to demonstrate that there had been no discrimination. Specific guidance should be provided on what comprises a situation in which there has been no discrimination, clarifying the requirements with which the data holder must comply.

(8) Article 13: Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise

There is an element of unpredictability in relation to data efficacy and the results that can be obtained from data use. Instituting a limitation of liability from the position of the data provider should not be considered unfair.

(9) Article 14: Obligation to make data available (to public sector bodies) based on exceptional need

- This provision obliges companies to share data with public sector bodies demonstrating an exceptional need to use the data requested, but we believe that data sharing should be conducted based on voluntary partnership.

Data held by companies is the product of innovation and investment, and concerns in relation not just to intellectual property rights but also to security and privacy mean that the introduction of a compulsory scheme could conversely constrain private-public partnership. Rather than a compulsory scheme, public sector bodies should consider providing legal and technical protection for data sharing by companies as well as incentives for companies to share data voluntarily.

- The European Council should create a clear and comprehensive EU list of situations comprising "exceptional need" and provide clarification through guidance, etc. Should a compulsory scheme be introduced, it will enable public sector bodies to determine when demand arises for data sharing based on exceptional need, with such unilateral judgements potentially creating legal uncertainty for companies. It is also unclear why small and micro enterprises have been excluded from this provision.

(10) Article 24: Contractual terms concerning switching between providers of data processing services

This provision sets out conditions in relation to switching between providers of data processing services, requiring that where the customer wishes to switch to a data processing service offered by another provider of data processing services, "full continuity" must be ensured. However, because specifications differ among data processing services in terms of the additional services provided, etc., there will be cases in which "full continuity" cannot be ensured. This language should be changed to "functional equivalence" in line with Articles 23, 26, and 29.

(11) Article 15: Exceptional need to use data

Article 15(c) appears to mean that this Chapter can be applied in cases of hindrance of the use of data for public duties provided by law. As there is no element of emergency need or public interest that justifies compulsory data collection in situations other than the public emergencies stipulated in (a) and (b), national governments and public sector bodies should conclude use contracts with companies.

(12) Article 20: Compensation in cases of exceptional need

Use of data created through company efforts free of charge or with payment proportionate to man hours in relation to (a) and (b) in Article 15 will reduce the incentive to create data. National governments and public sector bodies too should pay market price.

(13) Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs

Any additional use of data departing from the purpose of use when the data holder provided it should require new consultations, or at very least the payment of a corresponding additional consideration.

(14) Article 27: International access and transfer

- Article 27.1 appears to apply to the cross-border transfer of non-personal data in general.

It should be made clear that this provision is intended to prevent the unrestricted transfer of data in response to data transfer requests from the law enforcement agencies of third countries that are not based on international agreements.

- Concerns over data access by third-party governments ("government access") should be addressed not by requiring data processing service providers in the Cloud or on the edge to take measures but rather by considering measures in line with international standards and rules at multilateral government consultations such as the OECD.

(15) Article 35: Databases containing certain data

- This provision notes that the *sui generis* right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a connected product or a related service. We interpret this to mean that databases in which companies have made a material investment in data acquisition and indication of confirmation quantitatively and qualitatively and mixed databases containing data arising from the use of connected products and related services will not be protected. Because this provision could reduce companies' motivation to collect and share data, the scope of protection of the sui generis right should be further clarified.

# # # #