JAPAN INTELLECTUAL PROPERTY ASSOCIATION

Nihombashi 3-Chome Square Bldg.
6F, 9-1 Nihonbashi 3-chome,
Chuo-ku, Tokyo 103-0027, JAPAN

TEL:+81-3-6262-1570
FAX:+81-3-6262-5655
URL:http://www.jipa.or.jp/

May 13, 2022

European Commission
Charlemagne building
Rue de la Loi 170
1040 Brussels
Belgium

Re:JIPA Comments to 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)

We, the Japan Intellectual Property Association (JIPA), are one of the world's largest organizations of IP users with a membership of 1338 members (as of May 11, 2022), most of which are Japanese companies.

In light of the fact that our member companies expand business in Europe and have a great concern on “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, COM(2022) 68 final)”. Therefore, JIPA has carefully considered the new legislative proposal in February 2022 by European Commission. We, JIPA, respectfully submit our comments on the act and the rules, as below.

European Commission is kindly requested to take our comments into consideration when deciding on the revisions to the act and rules.

Sincerely yours,

Toshio ASAI	Hisashi ISHIJIMA	Toshihiko KOBAYASHI
Vice-President	Managing Director	Managing Director

(Contact) Ms. Maho Furuya : furuya@jipa.or.jp

I. Overview

Japan Intellectual Property Association (“JIPA”) has numerous member companies cross-sectionally covering all industry sectors, many of which have business operations on a global scale including European countries. These member companies are placed in the Data Economy in one or multiple positions of users, manufactures of products, suppliers of related services and data holders. JIPA expects that exploitation and use of data should lead the creation of innovation and the activation of businesses, and supports the aim of Data Act "ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data."

JIPA is convinced that in order to achieve the intended objectives of the Data Act and unlock the potential of data, it is necessary to minimize burdens of stakeholders (actors) on a fair balance and also respect economic values of important data possessed by companies in every aspect of the system. Further, intellectual properties possessed by companies, such as trade secrets, should be respected and protected under the provisions of the Data Act from imperilment in scenes such as accesses to data.

More specifically, the Data Act imposes heavy duties on manufacturers of products or data holders. JIPA concerns that obligations to provide data as a source of competitiveness to third parties, and human and financial burdens on companies caused by each obligation of the Data Act decline incentives to create or exploit/use data of companies, consequently leading to opportunity losses. Further, the cost required for fulfillment of the obligations is directly related to cost increases of data businesses. In view of the forgoing, if obligations imposed on companies are excessive, they rather give larger barriers to the development of data economy. In this regard, the Japanese Government promotes exploitation and use of data on a soft law basis and keeps obligations or limitations to the minimum, and respects free economic activities of companies. In order to "foster access to and use of data," we wish that the Data Act would provide a balanced system without imposing unfair, unreasonable or excessive burdens on each stakeholder.

In addition, as companies' properties that enable the promotion of existing businesses and the creation of new businesses, the value of data has increased every year. At the time of providing data, payment of an appropriate compensation based on its value ensures "fair allocation of value from data," giving an incentive for a favorable cycle in the creation of new data and the promotion of businesses using data. It is respectfully requested to design a system that respects the value of data possessed by a data holder through the Data Act.

In many cases, valuable data is protected with an intellectual property such a trade secret. A trade secret is also an important property of a company, and is a source of competitiveness. We put a high value on the situation where in Europe, EU Directive 2016/943 promotes the protection of trade secrets. With the premise that the protection of trade secrets should be sometimes prior to accesses to data, trade secrets should be sufficiently protected by the Data Act.

Hereafter, our opinions will be described on each article.

II. Particulars

1. Articles 1 and 2

(1) Scope of the Data Act

It is respectfully requested to clarify, in a more restrictive manner, data and products/services for which the Data Act is intended.

Paragraph (15) in the preamble of the Data Act says that servers, tablets and smart phones, cameras and others are excepted from the scope of the Products; however, it is difficult to clearly understand such exception from the definitions of the Products in Article 2. Further, "devices that require human input to produce various forms of content" is excepted from the scope of the Data Act, and human inputs may be also considered to be for automobiles, trains, smart factories and surveillance cameras; however, it is practically difficult to determine whether they are in the scope of the Data Act.

It is also unclear that platform services without use of a tangible object is excepted from the scope of the Data Act. In addition, we would like to clarify that cases where software is provided through a cloud or a platform (for example, software for accounting, business management or data analyses) is excepted. If these cases are interpreted to be covered, there is a concern that the applicable range of the Data Act is very and too broad.

Further, data that is discarded by data holders should be excepted.

In the case that data acquisition amounts are large, it is difficult to store and provide a huge amount of acquired data in real situations, and it is a business practice that is often performed to process data by edge-computing within products or related services just after acquisition of it and delete unnecessary data. Before deletion of unnecessary data, it may be possible to send all data on a real-time basis, but it is not realistic since a large data amount cause congestion on communication lines. It is respectfully requested to create appropriate rules in line with business practices, having interviews to collect opinions of industries.

Moreover, when the scale of a business operation is small regardless of the size of a company, obligations of the Data Act get to excessive burdens and may be obstacles to business. We believe that a business operation handling a certain amount of data or less should be exempt from the Data Act, and this avoids discouraging entering businesses and produces a balanced system.

(2) Applicable time range of data under the Data Act

Regarding contracts and data covered by the Data Act, it should be clear that data generated or acquired and contracts agreed before effectuation of the Data Act are exempted. Retroactive handling of old data or contracts before an effective date of the Data Act would impose excessive burdens on companies.

In addition, data that has been stored for a specified period after creation thereof should be exempt from the Data Act. A long period of storage imposes an excessive burden on companies in terms of the management and cost. Term of data storage obligation should be limited to reasonable period in the same manner as product liability.

2. Article 3

(1) The scope of data required to be provided

For the data accessible to the user, data intentionally recorded by the user himself/herself should be enough to provide.

Further, the place, the method and the timing of obtainment of data are a trade secret, and disclosure of such information would affect the competitiveness of a company. If a trade secret is publicized even once, its value would be lost; and therefore, in the case of a highly confidential trade secret, JIPA particularly and significantly concerns disclosure thereof. JIPA believes that a highly confidential trade secret should be except from disclosure obligation (e.g., Article 4, paragraph 3, and Article 5, paragraph 8). In addition, fulfillment of obligations of the Data Act, such as management and providing of data in a format that enables a user to be specified, and installation of a function of communication with users into the organization, imposes a heavy burden on a data holder. Thus, the period for obligations of the Data Act should be defined as a specified term and measures for preventing undue data request or abuse should be taken. As an exemplary measure therefor, it is considered that a data holder who discloses data is allowed to charge a certain degree of amount.

(2) Transitional measure

For this article, a transitional measure should be provided.

A penalty is applied to the violation of the article while preparations for fulfillment of the obligations are considered necessary. Thus, it is respectfully requested to provide a measure such as giving a certain period until the Data Act comes into effect or giving a certain period, during which a penalty is not applicable.

3. Articles 4 and 5

(1) Data providing to users

It is respectfully requested to clarify that the obligation of Article 4, paragraph 1 is an obligation in the case that a request is made by a user. Further, Article 4, paragraph 1 and Article 5, paragraph 1 impose heavy burdens on data holders, so they should be balanced.

As stated in the above proposal regarding Article 3, one of the obligations of the Data Act imposing heavy burdens on data holders is an obligation for data providing. The period of the obligation for data providing should be defined as a specified term and measures for preventing undue data request or abuse should be taken. As an exemplary measure therefor, it is considered that a data holder who discloses data is allowed to charge a certain degree of amount, and providing data free of charge should not be stipulated by law.

(2) Protective measure for trade secrets (Article 4, paragraph 3 and Article 5, paragraph 8)

"Specific necessary measures" for protecting trade secrets should be clarified.

It is not clear who defines "specific necessary measures" in what manner, and who determines whether or not the defined measure is sufficient as "specific necessary measures." Thus, we are concerned that an inappropriate application of the Data Act may occur such as a situation where a company is required to disclose a trade secret under an insufficient measure that is not agreed by the company.

As data is a source of competitiveness, JIPA believes that handling of data as trade secrets should be careful.

If a trade secret is publicized even once, its value would be lost; and therefore, in the case of a highly confidential trade secret, JIPA particularly and significantly concerns disclosure thereof. It is respectfully requested that a highly confidential trade secret should be exempt from disclosure obligation.

Further, in trade secrets, information are different from another information in terms of the importance or the management method, so specific contents of "all specific necessary measures" are not uniform and they are varied depending on the data to be provided. Thus, there is a concern that when the Data Act is applied in a rigid manner, an appropriate protective measure would not be taken. We respectfully request that appropriate protective measures for trade secrets would be taken under the Data Act.

In Article 4, paragraph 3, trade secrets shall be disclosed to the extent that the trade secrets are strictly necessary to fulfill the purpose in the same manner as in Article 5, paragraph 8.

(3) Range of use (Article 4, paragraph 6)

The range of use of data should be left to an agreement between the concerned parties.

In existing practices, the range of use of data is often defined by a contract according to the general rule that use of data is freely carried out unless otherwise agreed. However, if paragraph 6 allows use of data in only a range agreed with the user, the above general rule is reversed in such a manner that data shall NOT be used unless otherwise agreed. It is considered that such a limitation in exploiting and using data is unsuitable for the purpose of the Data Act and possibly discourages use and exploitation of data.

4. Article 6 (Article 6, paragraph 2, part (e))

Use and exploitation of data including use of data for competing products should be left to an agreement between the concerned parties.

In practice, it is difficult to distinguish a competing product from a non-competing product, so there is a concern that such a restriction would discourage use and exploitation of data. Services/products are often provided in combination of several products, and some of them may be used in a manner that was not expected during the development thereof and may be unintentionally used in a competing product.

5. Articles 7, 9 and 14

It is respectfully requested to design a system that is well-balanced between micro, small or medium enterprises and other companies.

We agree with the purpose of facilitating use and exploitation of data of micro, small or medium enterprises. On the other hand, when the Data Act is operated in an imbalanced manner, there is a concern that profits of companies other than micro, small or medium enterprises would be damaged irrationally.

6. Articles 8 and 9

(1) Conditions for data providing

We consider that FRAND obligation is not suitable for data transactions. Another criterion suitable for the purpose of the Data Act that allows stakeholders to fairly share data values should be established.

FRAND obligation is imposed after a FRAND license declaration on a technology pertaining to a standard specification to a standardization body. Since a standardization technology is concerned, the principle of freedom of contract is limited; however, data is not a standardization technology. Further, when FRAND obligation is imposed, especially, “non-discriminatory” obligation becomes a problem, making it difficult to provide data inexpensively or free of charge; and it impose to treat a competitor and a partner in the same way, therefore making it difficult to establish cooperation with the partner. In this manner, FRAND obligation prevents strategic and free handling of data for business operations.

(2) Compensation

A balance between the data holder and the user should be maintained.

While a wide range of data disclosure obligation is imposed on the data holder, the data holder is always required to indicate the basis for calculation of the compensation according to Article 9, paragraph 4; and this is a heavy burden.

We consider that the purpose of Article 9, paragraph 4 is fulfilled when the data holder indicates a reasonable basis for the compensation upon occurrence of a dispute.

(3) Exemption of data within one corporate group

Data transactions within one corporate group should not be treated in the same way as data transactions with a third party.

There are not a few instances where one business is operated in cooperation within one corporate group. Thus, when obligations of the Data Act pertaining to intercorporate transactions, especially FRAND obligation, are applied to transactions within one corporate group, this would be a great business concern.

7. Article 11

It is respectfully requested to clarify rules on the exception.

Regarding "significant harm to the data holder" and "disproportionate in light of the interests," criteria therefor are ambiguous, thus making it difficult to determine. Please provide specific examples in the preamble or the guideline.

8. Article 13

It is respectfully requested to explicitly stipulate that even when a data provider sets limitation of liability, the setting itself is not regarded unfair.

Results obtained by effects of data and use of data are unpredictable, and in practice, there are many cases where it is not suitable for a data provider to take responsibility for results of use and exploitation of data.

9. Article 15

Cases corresponding to "exceptional need" or "public emergency" should be clarified in a more limitative manner.

We have concerns that authorities would easily abuse requests for data providing requests. It is respectfully requested to clarity the circumstance therefor in such a manner that the data holder can objectively determine whether or not rejection of such a request is appropriate.

Further, the circumstance (C) should be deleted. This can be understood in such that this is applicable in many cases when impediments occur in the use of data during public services. However, cases other than "public emergency" are not urgent to put an obligation to provide data, and states or public sector bodies should conclude an individual contract with the data holder to receive data.

10. Article 19 (Article 19, paragraph 2)

It is respectfully requested to explicitly stipulate the responsibility including a compensation for a case where the data leaks from the authority having received those data.

Even though it is stipulated that an authority should take appropriate protective measures for protecting trade secrets and personal information, there is a possibility of leakage despite the protective measures. In the case that there is a risk that the inappropriate management of an authority causes the responsibility or the damage of the data holder, the data holder would hesitate to provide data if the responsibility of the authority is unclear.

11. Article 20

In the case that the data holder provides data to an authority, it is respectfully requested to compensate for a market rate or, if the market rate is not present, the amount including a cost incurred to comply with the request plus a reasonable margin.

In the case of public emergency (Article 15, part (a)), data shall be provided free of charge; however, no rational reason for free of charge is indicated, but the value of data produced by corporate efforts should be respected. Further, in a case where a company suffers some sort of loss along with the providing of data to the authority, for example, even a cost needed for the company to provide data cannot be recovered, JIPA concerns that data providing is not carried out smoothly and resulting the fear that data needed for the public interest cannot be provided swiftly.

12. Article 21

In the case that research organizations or the like use the data for usages other than the intended usage purpose of data determined at the time of providing the data, they should have separate talks on the conditions with the data holder or should pay an additional reasonable consideration.

13. Article 27

(1) Obligation of providers of data processing services

Since obligations on the provider are heavy, it is respectfully requested to reconsider them.

Obligations pertaining to international transfer or governmental access are imposed on the provider of data processing services, but cross-border circulation of data would contribute to the promotion of industries. These obligations on companies makes businesses in Europe and smooth cooperation with European companies difficult, resulting the fear that opportunities for creation of new businesses would be lost.

Further, if burdens on companies are heavy, only a limited number of large companies can deal with them, and this causes the fear that oligopolization of mega technology companies would be caused. Thus, placing obligations only on businesses handling a certain volume of data or more would promote use and exploitation of data and contribute to creation of new businesses.

Furthermore, users of data processing service are allowed to conduct, in the environment prepared by the provider, international transfers of data freely with no limitation as in conventionally done; and free cross-border transfers of data contributes to industries, and therefore, it is requested by all means to ensure free transfers.

(2) Access by governments

Providers of data processing services are obliged to take measures to prevent governmental access, but this obligation should be deleted. This is an excessive burden on one company, and we are concerned that this would be a significant hurdle for data processing services. This problem should be resolved by authorities of respective states.

(3) Consistency with the convention

Consistency with the convention should be taken into consideration.

Japan-EU Economic Partnership Agreement stipulates that "The Parties shall reassess within three years of the date of entry into force of this Agreement the need

for inclusion of provisions on the free flow of data into this Agreement." After its relationship with the Data Act is clarified, the consistency with inter-state agreements of this type should be maintained, and it is requested to cause no discrepancy.

14. Article 33

Penalties should be well-balanced not to discourage business activities.

Penalties possibly suppress use and exploitation of data, so toughening penalties should be avoided.

Further, specific contents of penalties are not determined in the Data Act. If penalties are varied depending on the state, this lowers the predictability or the transparency. If the Data Act lays down penalties, contents thereof should be concretely determined.

15. Article 34

(1) Operation of model contracts

Model contractual terms should be used flexibly in light of businesses.

Even when they are non-binding, rigid use of a model term in contract talks will prevent a smooth talk between concerned parties and thereby become an obstacle to businesses utilizing data.

(2) Process of formulating model contracts

For formulation of model contracts, it is respectfully requested to widely invite stakeholders to give their opinions.

Since there are many stakeholders for data, it is considered that the discussion should not be made only by the expert committee and gathering wide-range opinions enables the formulation of more practically useful model contracts.