JEITA's Opinion on the Proposed EU Data Protection Regulation
September 27, 2012
Japan Electronics and Information Technology Industries Association(JEITA)

1. Introduction

1.1 Overview of JEITA

- The Japan Electronics and Information Technology Industries Association, or JEITA, is an industrial association of Japan's typical electronics and information technology manufacturers, ranging from materials to electronic components and semiconductors, from consumer electronics to industrial system devices, from IT products to solution services.
- Its approximately 400 member companies are operating globally and their aggregate domestic and overseas turnovers amount to nearly 14 trillion yen and 26 trillion yen, respectively. Europe is one of the important centers for research and development, production, marketing, service, etc., and many member companies have established business sites there.
- Given the close relationship between Japan's electronics and information technology industries and Europe, the Proposed EU Data Protection Regulation released in January this year directly affects Japanese companies and their European affiliates as well, and JEITA would be pleased to be given the opportunity to give feedback on the proposed regulation.

1.2 JEITA's basic stance on data protection

- With the widespread use of the Internet and the advancement of ICT technologies, many companies are taking advantage of them to enhance their productivity, create innovations, and deliver new added value to people. In the public sector, these technologies are also used to create increased convenience, including the provision of new services to citizens and the enhancement of work efficiency. Furthermore, rapidly spreading SNSs are creating new personal links and various forms of communities.
- On the other hand, the distribution of large amounts of data across borders has increased the risk of data leakage, especially personal data, and the violation of privacy. We believe that the European Commission took timely action in response to these changes in the environment surrounding personal data as it reviewed the 1995 directive on data protection and presented a proposal for new data protection regulation.
- The protection and use of personal data have long been discussed from various angles on the regional, national and international levels, including at the OECD, due to the difference in history, culture, and the people's attitude toward personal data. However, in recent years, we have witnessed a global convergence of ideas about the principles of data protection. Given this international trend, we believe that there are three critical factors to personal data protection: (i) the protection of individual rights, (ii) the responsibility/accountability of companies and organizations, and (iii) enforcement by supervisory authorities. Japan's personal data protection framework should also be reviewed from this viewpoint.
- The proposed Data Protection Regulation recently released would be very welcome even by companies operating across Europe in that it reinforces the right of personal data protection, removes the detrimental consequences of national legislation variances among the European Union member states, and abolishes the obligation to notify supervisory authorities about the processing of personal data (general notification requirements). However, the new obligation that the proposed regulation impose on companies in order to safeguard data concerning EU residents could be enforced in a way that would cause relevant industries to bear new costs to ensure compliance with the regulation, with the result that the overall cost reduction claimed by the Commission would not be realized. The

proposal also contains a new rule whereby the EU regulation should also be applied to controllers in the case where data related to data subjects residing in the European Union and to whom products and services are provided is processed outside the EU.

- **Global data protection rules for companies operating in an environment where persons, goods, money, information, and other management resources are distributed across the borders (i) must be transparent and easy to understand, (ii) must be fair and harmonized both internally and externally, (iii) must be practical and effective, and (iv) must not impose excessive control on company activities or excessive burdens on companies. We hope that the release of the proposed Data Protection Regulation by the European Commission will trigger active discussion at the national or international agency level from the perspective described above and lead to the formation of an international framework concerning the protection and use of personal data that fits the modern social environment.**

2. JEITA's Opinion on the Proposed EU Data Protection Regulation

2.1 Transfer of personal data to third countries (Chapter V)

(i) On transfer to third countries and adequacy decision (related to Articles 39, 41, and 42)

- Article 41 of the proposed regulation allows for a decision on the adequacy concerning a processing sector within a third country, which we believe is preferable. Private companies in Japan safeguard personal data in accordance with the Act on the Protection of Personal Information as well as personal information protection guidelines issued by competent ministries and agencies. Japanese industrial associations will take action to convince the European Commission that Japan's private sector ensures an "adequate level of protection", in order to obtain a decision on adequacy for Japan as a whole or its private sector or certain industries.
- However, if an adequacy assessment application is filed by the Japanese government with the Commission, it will take some time to obtain a final decision. For the time being, Japanese companies have to receive personal data from controllers located within the EU (including Japanese companies' affiliates) in accordance with standard data protection clauses or BCRs (binding corporate rules). Article 42, paragraph 3 stipulates that standard data protection clauses adopted by the Commission or supervisory authorities "shall not require any further authorization". This can be interpreted to mean that Japanese companies do not have to obtain any further authorization from supervisory authorities when taking advantage of standard data protection clauses, implying a simpler procedure. We welcome such simplification of procedures concerning standard data protection clauses and BCRs in the proposal.
- However, controllers located within the EU may feel it burdensome to conclude standard data protection clauses with each non-EU company with respect to data transfer from the controllers, and this may lead to a loss of business opportunities for external companies. It would be detrimental to Japanese companies, especially those engaged in cloud services.
- Japan has the "Privacy Mark System" (a data protection seal), and more than 12,000 companies have already been certified under this system. JISQ15001 "Personal information protection management systems: Requirements", which governs the Privacy Mark, is based on the "Guidelines for the protection of personal information in the private sector", which were revised by the Ministry of International Trade and Industry (now the Ministry of Economy, Trade and Industry" in 1997 pursuant to the EU data protection directive. Thus, we believe that Japanese companies certified under the Privacy Mark system take appropriate safeguards equivalent to an "adequate level of protection". **We request that once Japan's Privacy Mark and European-level data protection seals as mentioned in Article 39 are mutually recognized, the Privacy Mark certification should be automatically**

taken as an adduction of "appropriate safeguards" as mentioned in Article 42, paragraph 1.

- Or the acquisition of the Privacy Mark or other data protection seals can be considered to be one of the criteria for making a decision on adequacy with respect to a processing sector within a third country. If this is the case, we request that it be clearly stated in the regulation, possibly a new sentence in Article 41, paragraph 2 about data protection seals.
- Globally operating enterprises are increasingly processing consumers' personal data across borders, and therefore need a data transfer method that is harmonized and standardized between countries and among regions. Thus, it is desirable that international standards concerning data protection be established in the medium-to-long term and harmonized with the EU Data Protection Regulation in terms of a decision on adequacy (Article 41) and appropriate safeguards (Article 42).

(ii) Transfer of employee data to third countries (related to Article 44)

- Many Japanese affiliates within the EU transfer only their employee data to head offices in Japan for legitimate purposes, such as the fulfillment of the employment contract. Because of the low possibility that individual rights are infringed in such data transfer, we request that the regulation expressly permit such data transfer, which is simpler than a transfer pursuant to standard data protection clauses or BCRs, on the condition that, for example, the data subject consents to such data transfer.
- It is, in fact, stipulated in Article 44, paragraph 1, point (a) that a data transfer is permitted if the data subject has consented to it. But what we are concerned about is that the employee's consent may not provide a legal basis for the employer to transfer the employee's personal data to a third country; this can be inferred from Article 7, paragraph 4, stating "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller", and from whereas clause (34), stating "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer in an employment context."

2.2 Extraterritorial application of the EU regulation (Article 3, paragraph 2)

(i) Conditions for exclusion from extraterritorial application

- We agree that the development of services supplied via the Internet has rendered it insufficient for the protection of personal data concerning EU residents to apply the EU legislation to non-EU controllers only in the case where data processing is conducted with equipment located within the EU, as stipulated in Article 4, paragraph 1(c) of the current EU data protection directive.
- However, in the case where, for example, an EU resident (including a Japanese national residing in the EU) happens to buy a product at a Japanese shopping site established by a Japanese company or happens to become a member of a Japanese social networking site operated by a Japanese company, it would not be reasonable to apply Article 3, paragraph 2 to such Japanese company. Of course, we believe that these cases are not subject to extraterritorial application, but non-EU companies would face a high degree of legal uncertainty unless it is expressly stipulated in what cases Article 3, paragraph 2 will be applied or not applied. Therefore, we request that the regulation expressly enumerate the conditions for excluding non-EU enterprises from Article 3, paragraph 2, including, by way of example, a statement on the website that the products and services

are not intended for EU member states.

2.3 Definition of personal data (Article 4 (1) and (2))

- In connection with the definition of the term "personal data", the proposed regulation refer to "location data" and "online identifier" as means of identifying an individual, which are not included in the current EU directive. And whereas clause (24) of the proposed regulation states "It follows that identification numbers, location data, online identifiers (such as Internet Protocol addresses or cookie identifiers) or other specific factors as such need not necessarily be considered as personal data in all circumstances", implying that in some cases these data, as such, may be considered to be personal data.
- In the case where private companies control Internet Protocol addresses, cookies, and other online identifiers in relation to individuals, it is possible to trace or profile the individuals online even if their names are not collected or stored by the companies. We agree that these data can be the subject of protection.
- However, the proposed EU Regulation do not clearly define in what circumstances these location data, Internet Protocol addresses, cookies, or other online identifiers (such as PC and smart phone identifiers) are considered personal data.
- The definition of the term "personal data" affects all the obligations of controllers (and processors) under the proposed regulation. For example, whether particular data is considered "personal data" or not greatly affects security measures for such data (Article 30), responses to the right to be forgotten (Article 17), the notification and communication of a personal data breach (Articles 31 and 32), and the imposition of a fine by the supervisory authority (Article 79). Therefore, if the scope of personal data is not clearly defined, it would mean significant legal uncertainty for the business activities of private companies.
- **As a representative of private companies, we request that the regulation clearly stipulate under what circumstances identification numbers, location data, online identifiers, or other "gray-zone" data will not be considered personal data, in other words, what kinds of measures controllers or processors should implement for such data in order to be exempted from the obligation to protect it as personal data when processing it.**
- For example, the report "Protecting Consumer Privacy in an Era of Rapid Change" released by the U.S. Federal Trade Commission in March this year defines protected data as "data that is reasonably linkable to a specific consumer, computer, or other device" and stipulates that data is not "reasonably linkable" to the extent that a company (1) takes reasonable measures to ensure that the data is de-identified (rendered anonymous or given a pseudonym), (2) publicly commits not to try to re-identify the data, and (3) contractually prohibits downstream recipients from trying to re-identify the data. This definition is very clear to private companies.

2.4 Lawfulness of processing and transparent policy (Articles 6, 7, and 11)

(i) Transparent policy and data subject's consent (Articles 4(8), 6.1, 7, and 11)

- We understand that because of the complexity and unintelligibility of the prevailing privacy policies of private companies, Article 11 of the proposed regulation imposes a new obligation of "transparency" on controllers, and because of the unintelligibility thereof that often renders data subjects' consents a mere formality, Articles 4(8) and 7.1 and 7.2 of the proposal require controllers to obtain explicit consents and Article 7.3 prescribes a new obligation to guarantee the right of data subjects to withdraw their consent.
- However, as private enterprises' data practices are becoming increasingly complicated and harder to

notice or understand for consumers, the more in detail privacy policies are written, the harder to understand and the more annoying they will be for consumers, possibly leading to the opposite result: consumers may mechanically "consent" without reading them carefully. In order to avoid such mechanical consents, it would be necessary to request individuals to carefully read the privacy policies and then give their explicit consent in all cases, but this would mean a significant burden and inconvenience to service users. **We need to identify a means for resolving this dilemma: if we try more to respect data subjects' consent and protect their individual rights, then their burden increases.**

- **In order to increase the transparency of privacy policies, it is preferable to classify the "purposes of data processing" for which the consent of the data subject is required into standard categories and ensure that these categories will be conspicuously indicated in privacy policies. The purposes of processing for which the data subject's consent is not required, such as those described in Articles 6.1.(b) to (f), should be allowed to be indicated in an inconspicuous way, e.g., on a page linked to the top page of a privacy policy rather than on the top page itself. However, if the purposes of processing for which the data subject's consent is not required, such as those described in Articles 6.1.(b) to (f), are not generally accepted ones or can be a surprise to individuals, then they should be indicated conspicuously.**
- **Further, the indication of data protection seals under Article 39 can be a good means to allow individuals to assess the lawfulness of data processing by private enterprises etc. We request that controllers who indicate such data protection seals be specially treated as meeting certain of the detailed transparency requirements that will be established under Article 11.**

(ii) Lawful processing of employee data (Article 7, paragraph 4)

- Article 7, paragraph 4 states "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller", and whereas clause (34) states "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer in an employment context." This can be understood as explaining that the employer, who is in a stronger position than employees, is prohibited to coerce employees into consent and process employee data (especially their race, ethnic origin, political view, region, genetic data, health and medical data, and certain other pieces of sensitive data) for illegitimate purposes.
- We can understand that employees' consent, in this sense, does not provide a legal basis for the processing of employee data by the employer. However, this explanation would mislead employers because it does not mention what they should do to ensure the lawfulness of employee data processing when it is done for the fulfillment of the employment contract or other legitimate purposes. **It seems that the lawfulness of employee data processing by employers when it is done for legitimate purposes is ensured by either Article 6.1.(b) "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract", or Article 6.1.(f) "processing is necessary for the purposes of the legitimate interests pursued by a controller". If this is the case, we request it to be clearly stated. Or if neither of the clauses can be interpreted to ensure the lawfulness of such processing, we request that the regulation specify what should be done to ensure lawfulness.**

(iii) Data processing upon the occurrence of a large-scale disaster (Article 6, paragraph 1)

If an earthquake, tsunami, or other large-scale disaster occurs, it would be necessary to provide or use personal data without the consent of the data subjects for the purpose of assisting disaster victims to rebuild their lives and promoting other reliefs in an efficient manner, but to the extent not detrimental to their individual rights and interests. **It seems that the lawfulness of data processing upon the occurrence of such large-scale disasters is ensured by Article 6.1.(d) "processing is necessary in order to protect the vital interests of the data subject" or Article 6.1.(e) "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". We request it to be clearly stated in the regulation so that controllers will have no doubt about it.**

2.5 Right to be forgotten and right to data portability (Articles 17 and 18)

(i) Right to be forgotten and to erasure (Article 17)

- The current EU directive also prescribes, in its Article 12, the right to have one's own personal data erased, but this right to erasure is not necessarily guaranteed unless there are good reasons, such as the inaccurate nature or illegal collection of the data. With the volume of personal data made public at social networking sites etc. increasing, the proposed regulation stipulates in its Article 17 that data subjects have the right to have their personal data erased if they withdraw their consent or upon the expiration of the storage period consented to. We understand this is great progress in the protection of personal data.
- However, while the scope of personal data required to be erased is mentioned in Article 17 ("personal data relating to them"), the scope of the term "personal data" itself is not clearly defined in the regulation as discussed in Section 2.3 above.
- It is also not clear if, when erasure requests are made by data subjects, information added by controllers, such as evaluations (credit status etc.) and medical information (charts, test results, etc.) concerning the individuals, must also be erased or may be excluded under Article 17.3.(d) ("for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject").
- **We interpret data rendered anonymous as not being required to be erased since whereas clause (23) states "The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable" and data rendered anonymous is not considered as "personal data".**
- **The scope of personal data required to be erased is very important for private companies to ensure their ability to respond properly to data subjects' erasure requests as they are received, when developing products and services involving personal data processing, in particular, designing personal data management methods. Therefore, we request it to be clearly defined in a delegated or implementing act.**

(ii) Right to data portability (Article 18)

- Article 18 appropriately prescribes an individual's right to transfer his/her own personal data from one service to another.

  However, the data that can be obtained in a certain format to protect an individual's right should be limited to his/her profile information (such as name, sex, age, address, photograph, hobby) and personal postings, and should not include log data, such as his/her site visit and purchase histories. These data are closely related to corporate

business models, and should private companies be required to give, at user requests, such data in a format which allows data portability to another service, they might be discouraged from creating innovative services. So, we hope that the portability requirement will not be an excessive one. We think the right of personal data protection with respect to such log data can be adequately secured by rendering such data anonymous or erasing them in accordance with Article 17.

2.6 Obligations of the controller and the processor (Chapter IV)

(i) Notification of a personal data breach to the supervisory authority and communication thereof to the data subject (Articles 31 and 32)

- Articles 31 and 32 require the controller/processor to notify personal data breaches to the supervisory authority and communicate them to the data subject. Such notification itself is a taken-for-granted duty of a company, and Japan's Basic Policy on the Protection of Personal Information also states "If the leakage of personal information etc. occurs, it is important for the company to disclose the fact etc. to the extent possible in order to prevent the occurrence of secondary damage, similar incidents, etc."
- However, it is very difficult for the company to fulfill the obligation of notifying the facts (the types and number of data leaked, the consequences of the leakage, measures to mitigate the possible adverse effects, and measures proposed or taken by the controller) to the supervisory authority, "where feasible, not later than 24 hours after having become aware of" the leakage. Given the fact that recent personal data leaks often involve millions of data stored in several databases, it would take some time to identify the scope of leakage and determine the future course of action (for example, in the case of malicious hacking, a technical investigation can be a time-consuming activity). **Although the controller should be required to give the first report on a personal data breach within 24 hours (specifying the type of the breach, a brief description of the then available information, and the data protection officer's contact details), we request that the detailed requirement prescribed in Article 31, paragraph 3 be replaced with a more practicable one: for example, the controller shall give a detailed notification to the supervisory authority without undue delay as soon as an internal authorization is obtained.**
- And not all data breaches necessarily pose a serious risk to the right of the data subject. Japan's Guidelines Targeting Economic and Industrial Sectors Pertaining to the Act on the Protection of Personal Information exempt companies from the obligation of notification to the competent minister (which corresponds to the supervisory authority) in the case of the "loss etc. of a commercial directory etc. that is easily available to anyone at a bookstore". Thus, **we request that the EU regulation expressly prescribe the cases in which companies are exempted from the obligation to notification to the supervisory authority and communication to the data subject because of the minor impact on the data subject.**

(ii) Data protection impact assessment (Article 33)

- Article 33 requires the controller etc. to assess the impact on personal data protection of the envisaged processing operations that can present specific risks to the rights of data subjects, which we think is appropriate for protecting personal data as well as for eliminating the need for companies to take "Bolt-on" measures, which mean additional costs to them.
- Article 34, paragraph 2 mentions a case in which the consultation of the supervisory authority is required in connection with a data protection impact assessment. If this prior consultation is a time-consuming process, private companies might have to postpone the commencement of the service involving the personal data processing operations at issue accordingly, and this might affect their

business activities. **We request that the supervisory authorities ensure, by establishing an appropriate mechanism or system, that such prior consultation will be completed promptly.**

- **Many Japanese companies collect employees' health data, including medical examinations, in order to promote their welfare. In this case, health data is not processed for taking measures or decisions regarding specific individuals (employees) as mentioned in point (b) of Article 33.2, and we request that a delegated act clearly stipulate that a data protection impact assessment need not be carried out in such case.**

(iii) Data protection by design and security of processing (Articles 23 and 30)

- Article 23 (Data protection by design and by default) and Article 30 (Security of processing) empower the Commission to adopt delegated or implementing acts for the purpose of specifying further technical standards and technical measure criteria. **We request that such standards and criteria established by delegated or implementing acts should be reasonable in light of the nature and size of private companies' business activities (cf. point (b) of Article 79.3), should take practicable technology application into consideration, and should not place an excessive economic burden on them. We also request that such standards and criteria be harmonized with international discussions and consensuses, including by private-sector standardization organizations.**
- **It is difficult to completely protect personal data from malicious attacks, including unauthorized access, with security measures. If a personal data breach, such as leakage, takes place as a result of an external attack, the company should still be regarded as having fulfilled its obligations as a controller or processor so long as it has taken reasonable technical measures as mentioned above.**

2.7 Fine by the supervisory authority (Article 79)

- Paragraphs 4 to 6 of Article 79 prescribe three fine rates to be imposed by the supervisory authority: up to 0.5%, 1%, and 2% of a private company's annual worldwide turnover. Although the regulation does not provide for a fine on a company's personal data breach itself (such as the leakage of personal data), a fine equal to up to 2% of its annual worldwide turnover will be imposed in the case of the failure to take appropriate measures in accordance with Article 30 (Security) or to notify a personal data breach to the supervisory authority in accordance with Article 31 or communicate it to the data subject in accordance with Article 32. This maximum amount is so large that it can endanger the existence of the company.
- Even if private companies have taken reasonable data security measures, it is still possible that their data is illegally accessed by malicious hackers. The more widely known a company is, the more attractive it may appear to such hackers. **Given these situations, the maximum fine of 2% of a company's annual worldwide turnover is too heavy, and we request that the maximum amount be stated as an absolute figure.**
- With respect to the determination of the amount of a fine, Article 79, paragraph 2 states "The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organizational measures and procedures implemented pursuant to Article 23 and the degree of cooperation with the supervisory authority in order to remedy the breach", but no specific calculation basis is set out. **It seems that Article 79 does not expect the Commission to establish further rules (such as delegated or**

implementing acts), but we insist that a specific calculation basis be defined in such further regulations or otherwise.

2.8 Certification mechanism and data protection seal (Article 39)

- Article 39 requires the member states and the Commission to encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, and empowers the Commission to adopt delegated or implementing acts for the purpose of further specifying the criteria and requirements for this purpose. There are already several certification mechanisms and data protection seals in place around the world (e.g., Japan's Privacy Mark), and they are working effectively. We hope that in the examination of European-level data protection certification mechanisms and seals, these existing systems, in particular, mutual recognition therewith, will be taken into consideration.

--- END OF DOCUMENT ---

JEITA's Opinion on the Proposed EU Data Protection Regulation (excerpted version)

September 27, 2012

Japan Electronics and Information Technology Industries Association (JEITA)

Given the close relationship between Japan's electronics and information technology industries and Europe, the Proposed EU Data Protection Regulation released in January this year directly affects Japanese companies and their European affiliates as well, and JEITA would be pleased to be given the opportunity to give feedback on the proposed regulation. (See also the whole JEITA's Opinion we attached.)

1. Transfer to third countries and appropriate safeguards (related to Articles 42 and 39)

- We request that the following point should be added to Article 42 paragraph 2, as "appropriate safeguards."

  "(e) certification of data protection certification mechanisms or data protection seals referred to in Article 39, obtained by the data recipient."

- We request that the following sentence should be added to Article 39 paragraph 2, after "in third countries."

  "and mutual recognition with existing data protection seal systems including in third countries."

- Japan has the "Privacy Mark System" (a data protection seal), and more than 12,000 companies have already been certified under this system. JISQ15001 "Personal information protection management systems: Requirements", which governs the Privacy Mark, is based on the "Guidelines for the protection of personal information in the private sector", which were revised by the Ministry of International Trade and Industry (now the Ministry of Economy, Trade and Industry" in 1997 pursuant to the EU data protection directive. Thus, we believe that Japanese companies certified under the Privacy Mark system take appropriate safeguards equivalent to an "adequate level of protection".
- We request that once Japan's Privacy Mark and European-level data protection seals as mentioned in Article 39 are mutually recognized, or once Japan's Privacy Mark is accredited as a data protection seal referred to in Article 39, the Privacy Mark certification should be automatically taken as an adduction of "appropriate safeguards" as mentioned in Article 42, paragraph 1.
- Article 39, paragraph 2 empowers the Commission to adopt delegated acts for the purpose of further specifying the criteria and requirements of data protection certification mechanisms and of data protection seals. There are already several certification mechanisms and data protection seals in place around the world (e.g., Japan's Privacy Mark), and they are working effectively. We hope that in the examination of European-level data protection certification mechanisms and seals, these existing systems, in particular, mutual recognition therewith, will be taken into consideration.

2. Conditions for exclusion from extraterritorial application (related to Article 3, paragraph 2)

- We request that the regulation expressly enumerate the conditions for excluding non-EU enterprises from Article 3, paragraph 2, including, by way of example, a statement on the website that the products and services are not intended for EU member states.

- In the case where, for example, an EU resident (including a Japanese national residing in the EU) happens to buy a product at a Japanese shopping site established by a Japanese company or happens to become a member of a Japanese social networking site operated by a Japanese company, it would not be reasonable to apply Article 3, paragraph 2 to such Japanese company. Of course, we believe that these cases are not subject to extraterritorial application, but non-EU companies would face a high degree of legal uncertainty unless it is expressly stipulated in what cases Article 3, paragraph 2 will be applied or not applied.

3. Transfer of employee data to third countries (related to Article 44)

- Many Japanese affiliates within the EU transfer only their employee data to head offices in Japan for legitimate purposes, such as the fulfillment of the employment contract. Because of the low possibility that individual rights are infringed in such data transfer, we request that the regulation expressly permit such data transfer, which is simpler than a transfer pursuant to standard data protection clauses or BCRs, on the condition that, for example, the data subject consents to such data transfer in accordance with Article 44, paragraph 1, point (a). Or we request it be clearly stated that such data transfer can be deemed “the transfer is necessary for the performance of a contract between the data subject and the controller” referred to in Article 44, paragraph 1, point (b).

- It is, in fact, stipulated in Article 44, paragraph 1, point (a) that a data transfer is permitted if the data subject has consented to it. But what we are concerned about is that the employee's consent may not provide a legal basis for the employer to transfer the employee's personal data to a third country; this can be inferred from Article 7, paragraph 4, stating "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller", and from whereas clause (34), stating "Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer in an employment context."

●Overview of JEITA

The Japan Electronics and Information Technology Industries Association, or JEITA, is an industrial association of Japan's typical electronics and information technology manufacturers, ranging from materials to electronic components and semiconductors, from consumer electronics to industrial system devices, from IT products to solution services. Its approximately 400 member companies are operating globally and their aggregate domestic and overseas turnovers amount to nearly 14 trillion yen and 26 trillion yen, respectively. Europe is one of the important centers for research and development, production, marketing, service, etc., and many member companies have established business sites there.

Appendix: Related provisions

Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) the offering of goods or services to such data subjects in the Union; or
(b) the monitoring of their behaviour.

Article 7 Conditions for consent

4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.

Article 39 Certification

1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.
2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.

Article 42 Transfers by way of appropriate safeguards

1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.
2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:
(a) binding corporate rules in accordance with Article 43; or
(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or
(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or
(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.

Article 44 Derogations

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:
(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or
(d) the transfer is necessary for important grounds of public interest; or
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or
(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Whereas clause (34)
Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.