OVERVIEW OF THE REVISED PERSONAL INFORMATION PROTECTION ACT OF JAPAN

Akira Matsuda
Iwata Godo

July 2020

On June 5, 2020, the House of Councillors of Japan passed the bill to amend the Act on the Protection of Personal Information ("APPI"). These revisions come as a result of the triennial statutory review process provided for under the APPI to give the legislator the opportunity to keep up with the rapid pace of innovation and technical change, and deal with the effects of the continuous expansion of the digital world and the ever-increasing volume of data handled by business operators.

Part 1 is an overview of the main amendments and Part 2 provides information on the timing of entry into force.

The English translation of the new legislation can be accessed through the link below.

https://www.ppc.go.jp/files/pdf/20200612_comparative_table_amended_APPI.pdf

Contents

1. OVERVIEW OF THE AMENDMENTS 1

2. TIMELINE AND IMPLEMENTING RULES 5

Inquiry contact:
newsmail@iwatagodo.com

1. OVERVIEW OF THE AMENDMENTS

1 More Rights for Data Subjects and Stricter Rules for Business Operators

The amendments introduce a number of measures aiming to give more rights to data subjects and stricter rules (tougher restrictions and prohibitions) from a business operator's standpoint. These measures are summarised below.

Enhanced Rights for Data Subjects and Stricter Rules	
(I)	Relaxed conditions for data subjects to demand cessation of use, deletion, and cessation of third-party transfers
(II)	Data subjects' right to choose their retained personal data disclosure method (and expansion of the scope of data to be disclosed)
(III)	Redefining "retained personal data": suppression of the short-term data exemption for data deleted within 6 months
(IV)	Third party transfers without consent: stricter opt-out exemption rules
(V)	Mandatory reporting of the leakage of personal data to the data protection authority (Personal Information Protection Commission (PPC) and mandatory notification to data subjects (subject to thresholds)
(VI)	Introduction of a new category of "Personally Referable Information" subject to specific third-party transfer restrictions under certain circumstances.

With respect to (I) above, under the current APPI, data subjects are entitled to demand (i) the cessation of use and deletion only in cases of violation of the purpose of use restrictions or acquisition of data by deceit or through improper means, and (ii) the cessation of third-party transfers only in cases of violation of transfer restrictions (for example, the requirement to obtain the consent of the data subject). In contrast, under the amended APPI, data subjects will be able to demand the cessation of use, deletion or cessation of third-party transfers when their rights or legitimate interests are likely to be infringed. Examples include cases where the business operator no longer needs the personal data in light of the purpose of use, or where substantial data breaches have occurred.

With respect to (II) above, (i) data subjects will be entitled to specify the method of disclosure (currently by delivery of written documents), and (ii) the scope of disclosures will be broadened to cover records of third-party transfers and receipts. The intention behind (i) is to encourage disclosure by way of electronic means and, accordingly, to reduce the administrative burden of the businesses when handling personal information. In certain cases, including where the specified method is very costly, the conventional method of disclosure using printed materials will continue to be allowed. As a result of the combination of (i) and (ii), violations of the confirmation and recording obligations will certainly come under the spotlight, as has been observed in the EU under GDPR.

With respect to (III) above, the exemption from the disclosure obligations under the current APPI for personal data prearranged to be erased within 6 months from acquisition (due to the definition of the expression "Retained Personal Data" which excludes such short-term retention) will be abolished. Accordingly, businesses will no longer be allowed to escape their disclosure obligations by erasing personal data promptly and will be required to comply with disclosure request by data subjects regardless of the period of retention.

With respect to (IV) above, the revision further limits the scope of personal data that can be provided to third parties without the data subject's consent based on the opt-out exemption by excluding (i) data illegally obtained and (ii) personal data received from another business operator based on an opt-out scheme.

With respect to (V) above, businesses must report data breaches to the PPC if conditions to be specified in sub-legislation are met (significant risk of infringement of an individual's rights and legitimate interests). In cases of leakage of information by an entrusted entity (the processor), the entrusted entity will be exempted from the reporting obligation if it reports it to the entrusting entity (the controller).

Furthermore, in case of mandatory reporting to the regulator, businesses will in principle also be required to notify data subjects. The rule will be clarified in sub-legislation, but will not apply to cases where notification to the data subject is difficult and the necessary alternative action is taken to protect the rights and interests of data subjects.

With respect to (VI) above, the amendments will create a new database category called database comprising "Personally Referable Information". Personally Referable Information (PRI) is defined as information which neither qualifies as Personal Information, Anonymously Processed Information nor Pseudonymously Processed Information, but fulfils conditions set out below. The consent of the data subject will be required, if the information concerned (i) relates to a living individual and is systematically organized to constitute a database, and (ii) will be acquired by a third party as personal data in the course of the provision of such PRI database to the said third party. In other words, PRI is not information enabling the identification of an individual person for the transferring party, but is treated as information enabling the identification of an individual person for the receiving party.

The business which acquires a PRI database by way of third-party transfer will also be obliged to confirm that the consent of the data subject has been obtained.

Although the PRI regulations are quite complex, they are intended to cover the following cases excluded from the consent requirement under the current APPI:

Case (1)

Company A, which is engaged in the business of supporting job seeking students, acquires and retains the cookie information of the job seeking students who visit its website. Such cookie information is insufficient to identify a specific individual either by itself or combined with other information retained by Company A. Company A provides such cookie information to its clients, which are companies contacted by job seeking students.

Company A was aware of the fact that client companies were able to identify a specific individual by collating cookie information provided with other information held by them. Company A provided client companies with the job offer rejection rate of holders of certain cookie information. As mentioned, the job offer rejection rate is, for Company A, information which is insufficient to identify a specific individual; however, it allows client companies to identify a specific individual to whom the rate corresponds.

Company A did not obtain the consent of the job seeking students in respect of the transfer of the cookie information of such job seeking students to Company A's clients.

Case (2)

Company B, a targeted advertising service provider, obtains from DMP (Data Management Platform) operators certain data which is insufficient to identify a specific individual at DMP's end such as attributes and preferences together with the corresponding cookie information which was created upon obtaining

the data (the DMP operators are unable to identify a specific individual even if they combine such data with the cookie information).

Company B, by using the cookie information as a hub, combines such data provided by the DMP operators with the personal information of its own customers that it retains (such as purchase history, access logs, and navigation analysis) to conduct segment analysis and customer profiling, based on which targeted advertisements will be generated.

The DMP operators are aware of the fact that the information provided by them to Company B will be utilized at Company B's end in a manner which allows the identification of a specific individual. The DMP operators have not obtained the consent of the data subjects with regard to the provision of such information to Company B.

2 Other Amendments

The amendments also seek to facilitate data usage, extend the extra-territorial scope of the APPI, and strengthened sanctions (penalties).

Other Amendments	
(I)	Introduction of a new category of “Pseudonymously Processed Information” (PPI)
(II)	The reporting and disclosure obligations will also apply to operators located outside Japan if they handle personal data of an individual located in Japan (administrative penalties would be imposed for breach of such obligations).
(III)	Broader information disclosure requirements for cross-border transfers of personal data • Businesses transferring personal data overseas based on the consent of data subjects, will be required to provide the data subjects with certain information (such as an overview of the personal information protection rules of the country in which the receiving entity is located) before obtaining their consent,. • Businesses which rely on binding corporate rules or data transfer agreements for their transfers of personal data to an entity outside Japan, will be required to provide the data subject with certain information regarding the manner of the receiving party's handling of personal information on request of the data subject.
(IV)	Stricter sanctions • The fine for violation by a company will be increased to up to JPY100 million. • No administrative surcharge scheme will be introduced (subject to further discussions).
(V)	Discussed but not introduced this time: • Mandatory Privacy Impact Assessment scheme • Mandatory requirements for Data Protection Officers

PPI under (I) above is a new category of information created in-between Anonymously Processed Information and Personal Information as information that can only identify a particular individual by collating it with other information. Information falling within this category, processed in such a way that it is not possible to identify a specific person, by pseudonymising part of it while keeping the key to restoration as personal data, will be exempted if such information is (i) to be used only internally and for certain purposes such as analysis, and (ii) the purpose of use of PPI is specified and published. Third-party provision of PPI will be prohibited unless otherwise specifically provided by the relevant laws and regulations.

2. TIMELINE AND IMPLEMENTING RULES

Publication of the related sub-legislation and guidelines is scheduled as follows:

Summer 2020	Announcement on policies for administrative orders, rules guidelines and FAQs
Winter 2020	Public comments for administrative rules and orders
Spring 2021	Announcement of administrative rules and orders
Summer 2021	Announcement of guidelines and FAQs
Spring 2022	Entry into force of the amendments (part of the amendments will be in force earlier)

Akira Matsuda TEL: +81 3 3214 6282 E-MAIL: amatsuda@iwatagodo.com

Akira Matsuda is a partner at Iwata Godo and head of the Data Protection and AI/TMT practice group. He is an attorney-at-law admitted in Japan and based both in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions and capital markets, as well as international disputes (litigation/arbitration). Mr. Matsuda is also advising many Japanese and foreign clients on data protection and data security issues (Japanese laws, Singapore PDPA, and GDPR) and on the structuring of global compliance systems.

Mr. Matsuda is a graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

<Recent Publications>

- Data Protection 2nd Edition Country Comparative Guide (Legal 500)
- Global Data Review- Handbook 2020 (Data Privacy) (Law Business Research)
- Data Privacy & Transfer in Investigations (Global Investigations Review (Law Business Research))
- Global Legal Insights to: AI, Machine Learning & Big Data 2020 (Global Legal Group)
- Why AI is the future of Cyber Security (ICLG Cybersecurity 2020) (Global Legal Group)
- Corporate Investigation (Japan) (ICLG Corporate Investigations 2020) (Global Legal Group)

IWATA GODO

IWATA GODO
Established 1902

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with about 80 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection.

Marunouchi Bldg 15th floor, 2-4-1 Marunouchi, Chiyoda-ku, Tokyo, Japan www.iwatagodo.com/
E-mail: newsmail@iwatagodo.com Tel: +81-3-3214-6215