THOMSON REUTERS

Are you ready for the amended Japanese privacy law?

By Yukihiro Terazawa, Kyoko Sato and Kosuke Kunimine, *Morrison & Foerster*

JUNE 2, 2017

There are important changes to the privacy rules in Japan that affect the ways in which companies handle personal information, particularly with respect to disclosures to third parties, international transfers, and the collection and use of sensitive personal information.

These changes are the result of amendments made to Japan's Personal Information Protection Act ("PIPA") in 2015, which entered into full effect on May 30, 2017.

The amendments to PIPA ("Amended PIPA"), which occurred more than ten years after PIPA was originally enacted, are intended to accomplish two key goals: enhance the protection of personal information, with a view to making such protections comparable to those provided by EU law, and promote effective and broader use of personal information by introducing new systems such as those for "anonymously processed information".

The Cabinet Order and Commission Rules for the Amended PIPA have also been finalized last year. In addition, the Personal Information Protection Commission (the "PPC") issued several guidelines as explained below.

An English translation of the Cabinet Order is available at http://www.ppc.go.jp/files/pdf/Cabinet_Order.pdf. An English translation of the Commission Rules is available at http://www.ppc.go.jp/files/pdf/PPC_rules.pdf.

Under the Amended PIPA, while there are some exceptions, organizations are required to obtain express consent from the individual at the time Sensitive Information is collected.

MAJOR CHANGES OF THE PIPA

The following items are the major changes to the PIPA, which will affect companies' personal information handling practices.

Before the Amended PIPA takes effect, Japanese companies handling employees' and/or customers' personal information in Japan may need to revise their privacy policies and/or data transfer agreement with foreign entities, such as affiliates or parent companies and/or outsourcing vendor located outside of Japan.

The good news is the Amended PIPA does not have retroactive effect.

Sensitive information

The Amended PIPA introduced a new concept of "Sensitive Information" which, until now, was found only in some sectoral guidelines such as the Guideline on the Protection of Personal Information in the Financial Sector (the "Financial Sector Guideline").

The Amended PIPA defines "Sensitive Information" as information on race, creed, social status, medical history, criminal records, victimized history, and other information provided in the Cabinet Order that may cause social discrimination.

The Cabinet Order further provides a detailed definition of the Sensitive Information that includes physical, intellectual, and mental disabilities, and the results of medical checkups.

Under the Amended PIPA, while there are some exceptions, organizations are required to obtain express consent from the individual at the time Sensitive Information is collected.

Because organizations routinely collect this type of information for human resource purposes, Japanese companies may need to revise their privacy policy in which employees agree that the employer will collect and use their sensitive information for specific purposes and ask their employees to agree with their revised policy.

Disclosures to foreign third parties

The Amended PIPA introduces a new rule for transferring personal information to foreign third parties, which includes a parent company or affiliated companies and/or outsourcing vendors located outside of Japan.

While there are some exceptions, express consent or a data transfer agreement/intercompany policy or rules applicable to all of group companies will be required unless the transfer is to a third party:

- In a country that is designated by the PPC to have legislation on personal information protection that is considered to be equivalent to that of Japan; or
- That has an internal personal information protection system that is equivalent of what PIPA requested.

Because the PPC has not yet designated any countries "equivalent", Japanese companies may wish to (a) obtain consent from individuals (e.g. employees and/or individual customers); (b) execute or revise a data transfer agreement or intercompany policy or rules which implement a personal information protection

system that meets the requirements established by the PPC; or (c) confirm that a foreign transferee has obtained a certificate that it complies with APEC CBPR System.

Prior notification to the PPC in using opt-out consent

Currently under PIPA, organizations may provide personal information to third parties without obtaining the individual's express consent if they provide prior notice to the individual or place a notice in a location that individuals may easily access it.

The notice must contain the following information: (i) third party transfer is one of the purposes of use; (ii) the items to be transferred to third parties, (iii) the manner in which information is transferred; (iv) the right to request that information cease being transferred (i.e. an opt-out right); and (v) how the method by which an individual can communicate that choice.

> Data breach notification is not explicitly addressed in the Amended PIPA but is addressed in some of the ministry guidelines.

The Amended PIPA introduces an additional requirement to provide a similar notice to the PPC (i.e. regulatory notice) ("opt-out notification").

The PPC started accepting such notices effective March 1; however, enforcement of this new notification requirement began May 30, 2017.

Please note that organizations are prohibited from providing Sensitive Information to third parties using an opt-out scheme.

Record keeping obligation

The Amended PIPA introduces new record keeping obligations.

Organizations will be required to maintain a record of their third party data transfers, noting:

- The date of the transfer (based on an opt-out scheme);
- The names of the transferees;
- The name and other information that may identify individuals;
- Items of personal information provided or received;
- The fact that consent of the individual has been obtained (for those transfers that are based on the consent of the individual); provided, however that such record will not be required if the transferee is located within the territory of Japan and
- An organization provides personal data to a service provider to carry out services (e.g., outsourcing vendor of HR services or IT services);
- An organization provides personal data to a third party (e.g., acquiring company) in connection with a merger or acquisition; or
- An organization shares such personal data with a third party (such as the parent company) and informs individuals of the items to be shared, the scope of such third parties, the purpose of the share use, and the name of a person responsible for the management of such personal data or puts such information in a place that individuals may easily access it.

The Amended PIPA also requires keeping a record of personal information received from third parties, noting:

- The date of the receipt (for data received under an opt-out notification scheme);
- The names of the transferors;
- Background information regarding how the transferee acquired the personal information;
- The name and other information that may identify the individual;
- Items of personal information provided or received;
- The fact that the notification of data transferred on the basis of an opt-out has been provided to the regulator;
- The fact to the effect that consent of the individual has been obtained (for those transfers that are based on the consent of the individual).

Please note that, in addition to the exception described above, there are other exceptions for the record keeping obligations.

Anonymized processed information

The Amended PIPA and the rules issued by the PPC create new requirements for the creation and use of anonymized processed information.

If a company deletes certain information that may identify individuals from personal information and creates anonymized processed information in accordance with the amended PIPA, the company may use anonymized processed information for any purposes and transfer such anonymized processed information to any third parties.

A company that anonymizes data, however, must take the following steps, including:

- Publicly announcing the items of information that will remain anonymized (such as age, gender, and/or residential area);
- Establishing internal rules to avoid divulging the process of anonymization; and
- When transferring anonymized information to a third party, publicly announcing the items of information included in the anonymized information to be provided and the method of the provision, and notifying the third party that the transferred information is or contains anonymized information.

While those rules do not apply to the receiver of such anonymized information, the receiver/users of such anonymized information (i.e., a company having data base containing anonymized information) may not try to re-identify the data.

The Amended PIPA prescribes penalties in certain circumstances, however, such penalties would not be applied to companies or individuals if it simply violates the Amended PIPA.

ENFORCEMENT

Establishment of the personal information protection commission

Currently, each competent Minister supervises protection of personal information for each industry.

For example, the Ministry of Economy, Trade, and Industry supervises a broad array of industry sectors such as manufacturing and retail while the Financial Services Agency supervises the financial services industry.

Each Ministry has the authority to require reports from business operators regarding their handling of personal information, provide advice and issue recommendations concerning law violations and necessary corrective measures, and issue orders in the event that their recommendations are not adopted by the business operator.

Once the Amended PIPA fully comes into force on May 30, 2017, all of the enforcement powers previously assigned to the individual ministries will be transferred to the PPC and the PPC will become the central enforcement authority for all sectors except the financial sector.

In addition, the PPC will have the ability to conduct on-site inspections.

Data breach notification obligations

Data breach notification is not explicitly addressed in the Amended PIPA but is addressed in some of the ministry guidelines.

For example, the Guidelines on Protection of Personal Information in the Financial Sector, the Guidelines on Protection of Personal Information in the Credit Segment, and the Guidelines on Protection of Personal Information in the Loan-Servicing Sectors require business operators to report to the regulators information regarding data breaches and remedial measures taken in the event of a leakage of personal information.

Although the Amended PIPA does not impose a legal obligation on organizations to notify governmental agencies in the event that personal information is leaked, the PPC has issued guidance applicable to all sectors that recommends that business operators report relevant facts and remedial measures to the PPC (or competent minister if so specified by the PPC) in the event of a leakage, loss, or damage of personal information, except for some minor incidents (e.g., if there was no substantial harm because the leaked information was retrieved before it could be reviewed by third parties).

Data breach reporting forms will be available on the PPC website of the PPC in the near future.

Penalties

The Amended PIPA prescribes penalties in certain circumstances, however, such penalties would not be applied to companies or individuals if it simply violates the Amended PIPA.

For example, if a company transferred personal data to a foreign company without obtaining consent of individuals, such company will likely not be penalized under the Amended PIPA.

Please note, however, a company that violates the Amended PIPA may be sued by an individual and/or the PPC may initiate an investigation and issue an administrative order or recommendation against a violating company.

The Amended PIPA does impose a penalty on a business operator or its employee (including former employee) who steals or misappropriates personal information.

Those penalties include imprisonment of not more than 1 year or a fine not more than 500,000 yen.

Past enforcement

The number of enforcement actions on an annual basis is decreasing.

Since the enactment of the law, there have been no orders or penalties issued, largely because Japanese companies tend to comply with the PIPA and abide by advice and recommendations from regulators.

The most serious case to-date occurred in 2014 when the Benesse Corporation, an education service provider, suffered a data breach that affected 48.6 million customers.

Citing Benesse's lax security procedures and inadequate supervision of personnel, the Ministry of Economy, Trade, and Industry issued a recommendation requiring Benesse to take responsibility for the actions of its business partners, increase management attention to data security, and ensure that its data protection administrative structure was in place. Fines or other penalties were not issued.

It is unclear whether the PPC intends to take a similar enforcement approach once the Amended PIPA goes into effect.

CONCLUSION

The regulations and guidance relating to the Amended PIPA are voluminous. Companies should ensure that they are familiar with the obligations and prepare to comply.

This analysis first appeared in the May June 2, 2017, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHORS



Yukihiro Terazawa (L) is a partner in the Tokyo office of **Morrison & Foerster** and a member of the firm's intellectual property and privacy and data security groups. He can be reached at yterazawa@mofo.com. **Kyoko Sato** (C) is an associate in the Tokyo office of the firm. She can be reached at ksato@mofo.com. **Kosuke Kunimine** (R) is an associate of the firm in Tokyo. He can be reached at kkunimine@mofo.com. A version of this article first appeared May 16 as a client alert. Republished with permission.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.