New amendments to Japanese privacy law

Data Protection Alert

18 SEP 2015
By:

The Act on the Protection of Personal Information (the "APPI"), which was enacted in 2003 and which went into full effect in 2005, has not been amended since. Over the following decade, the advent of "big data" and the cross-border handling of information (particularly through cloud services) has had the effect of aging the APPI and shifting it out of line with internationally accepted standards. Further, recent scandals such as the East Japan Railways Company (JR) sale of customer data collected through the use of Suica cards have increased public awareness of the need to have clear standards for data disclosures. Japan's privacy laws have also faced growing criticism from the international community, as they are not up to the level required under the EU directives on privacy protection or the privacy laws of other jurisdictions.

All of these concerns coalesced into a bill passed by the Japanese Diet, to amend the APPI to address these and other issues (the "Amendments"). Unfortunately, the Amendments delegate most of the details of these broad policy objectives to a newly-created Privacy Protection Commission (the "Commission"). Until the Commission issues notifications on these issues, compliance with these Amendments will remain somewhat murky.

The following are the key points in the Amendments to the APPI, along with an explanation of how these changes will affect businesses handling this type of information.

Information protected by the APPI

The Amendments clarify some of the information classified as "personal information" under the APPI, and add two new classes of information: "sensitive information", the transmission of which has greater restrictions; and "anonymized information", which can (with certain restrictions) be transmitted without the express consent of individuals.

Clarification of "Personal Information"

The APPI had defined "personal information" as information regarding a living individual that contains an identifier of that individual, such as the person's name or date of birth. This includes information which, if connected with other information, could easily result in the individual being identified.

The Amendments maintain this definition but clarify that it includes any "personal identifier code." A personal identifier code refers to any biometric data that identifies a specific individual, or any code uniquely assigned to an individual with respect to the receipt of goods or services, or instruments (such as credit cards) with which to purchase such goods or services. Typical examples would be passport numbers or driver's license numbers. The exact details of what constitute a personal identifier code has been delegated to the Commission, which will publish details at some future point.

Based on the definition, it appears that the personal identifier code will only include codes assigned to individuals, rather than network devices or equipment, and therefore not include serial numbers for hardware or network addresses. However, as serial numbers or network addresses can sometimes be traced to a specific individual, it is possible that these would be considered personal identifier codes under the Amendments. When the Commission publishes its guidelines, it should provide more clarity on points such as this.

Addition of "Sensitive Information"

The Amendments introduce a new concept into the APPI: sensitive information. Sensitive information includes information about a person's race, creed, social status, medical history, criminal record, any crimes a person has been a victim of, and any other information that might cause the person to be discriminated against. The provision of sensitive information to third parties is subject to a higher level of scrutiny. Additionally, the "opt out" option (discussed below) is not available for sensitive information--prior consent is required from the party whose sensitive information would be given to a third party.

Addition of "Anonymized Information"

In addition to sensitive information, the Amendments also add to the APPI the concept of anonymized information. "Anonymized information" refers to any information about individuals from which all personal information (i.e., the information that identifies a specific individual, including any sensitive information) has been removed. As noted above, personal information includes personal identifier codes, so these must also be removed before information is considered anonymized. Companies must ensure that the personal information cannot be restored, although how companies can achieve this has been delegated to the Commission.

If a company has sufficiently anonymized the information, it can be disclosed to third parties without requiring the consent of the individuals whose personal information has been removed from the documents. However, care must be taken in anonymizing the information before disclosure; a failure to completely sanitize the information could result in the disclosure of personal information. Additionally, before disclosing the anonymized information to a third party, a company must publicly state (likely in its privacy policy) the nature of information included in the anonymized information, and the means by which it is sharing the anonymized information. Finally, the Commission has been tasked with instituting rules for disclosure, including the standards of anonymization.

Data transmissions

"Opt Out"

Currently under the APPI, with some exceptions, the transmission of any personal data requires the advance consent of the person whose personal information is to be transmitted. The individual must "opt in" before a company can share the personal data. The Amendments create a way for companies to share personal data with third parties, without needing to obtain the prior consent of individuals. The individual must "opt out" if he or she does not want a company to share the personal data.

With the Amendments, a company can now disclose personal data to a third party without the individual's consent if the following are publicly disclosed:

- the purpose of use includes the provision of such information to third parties;
- the nature of the personal data being provided to third parties;
- the method by which personal data is provided to third parties; and
- the method for an individual to submit an opt out request to the company.

If the individual does ask to opt out, the company must comply with this request.

In addition to the public disclosure requirements, if a company seeks to have "opt out" as the default, it must provide advance notification to the Commission that it is doing so. Additionally, if the company changes the nature of the personal data being provided to a third party or the means by which it is providing the personal data, it must notify the Commission of the changes. The Commission will publicly disclose the notification.

Whether this "opt out" option will have a practical effect on the sharing of personal data with third parties is unclear. It may still be easier for companies to rely on the "opt in" option, provided that the contractual language has been

sufficiently drafted.

Overseas transmissions of personal information

With the globalization of businesses, and the frequent use of cloud services, the transmission of information across national borders has become a common and integral part of businesses. Currently, the APPI has no provisions specifically governing the transmission of data outside of Japan. Although the provisions prohibiting data transfers could theoretically apply to overseas transmissions, the APPI's limitation on extraterritorial application has rendered it practically ineffective.

The Amendments specifically provide that a business entity must obtain the prior consent of any individuals whose personal information will be provided to a third party located in a foreign country. The "opt out" option will not be available unless the foreign country has similarly adequate standards for privacy protection. Whether the foreign country has such standards will be a determination of the Commission. Notably, an affiliated entity in a foreign country is considered a "third party" under the Amendments. However, branch offices (which are not legal entities) located in foreign countries are not a "third party" for purposes of the consent requirement.

De minimis exemption

The APPI included a de minimis exemption for any business whose database contains the personal information of 5,000 or less individuals in the prior 6 months. The Amendments remove this de minimis exemption.

Bookkeeping and verification obligations

The Amendments provide that a company which transmits personal data to a third party must maintain records of these data transmissions, including the date of the transmission and the name of the recipient. The Commission will determine what other records must be kept, as well as how long the records must be maintained.

Further, the Amendments require a business entity that receives personal data from a third party to verify the name and address of the third party, as well as how the third party obtained the personal data. The purpose of this requirement is to add a level of transparency to the traceability of transmitted data.

The Amendments' bookkeeping and verification requirement only applies to the transmission of personal data. Even the transmission of data containing the personal information of one individual that is part of a database could fall under this requirement. In the legislative discussion on the Amendments, the legislature explained that the bill does not intend to impose excessive requirements, but data processors should be mindful of this requirement.

Penalties for violating the APPI

Currently, the APPI does not include any punishment for illegal disclosures of personal data to third parties, either by a business entity or its officers and employees. The Amendments add a criminal penalty provision to the APPI. An unauthorized disclosure of personal information, for the benefit of the disclosing party or any third party, will be subject to a penalty of imprisonment for up to one year or a fine of up to JPY 500,000. If the party making the disclosure is a legal entity, the parties subject to this penalty will be the relevant officers, representatives, or managers responsible for the disclosure.

Creation of the Privacy Protection Commission

The Amendments create the Privacy Protection Commission (the "Commission"), which will act as a supervisory governmental organization on issues of privacy protection. The Commission, as noted above, has also been tasked with providing many of the details necessary to bring the Amendments into effect.

Currently, privacy protection is managed by each of the ministries that supervise the various industries of the private sector. Each of these ministries has adopted its own guidelines for privacy protection, which has led to overlapping and conflicting rules. The Commission is expected to bring these guidelines into alignment.

The Commission will be neutral and independent, and it will have the power to enforce the APPI. It is expected to adopt a more transparent and consistent approach to enforcement than what is currently in place with the various

ministries. However, it will only have the right to perform audits and issue cease and desist orders; it will not have the power to impose administrative fines.

If you have any queries or concerns about data privacy laws in Japan or elsewhere, our data privacy team, comprising of 130 data protection lawyers around the globe, would be pleased to hear from you.