Insight

IN-DEPTH DISCUSSION

JULY 5, 2017

Amendment to Japan's Omnibus Data Protection Law Means New Compliance Requirements for U.S. Multinational Employers With Operations in Japan

BY AKI TANAKA, TRENT SUTTON, AND PHILIP GORDON

Effective May 30, 2017, Japan amended its omnibus data protection law, the Personal Information Protection Act ("PIPA"), to add new compliance requirements that will have an immediate impact on many U.S. multinational employers with employees in Japan. As with the European Union's recent revamping of its data protection regime through the General Data Protection Regulation, which will go into effect on May 25, 2018,[1] the amendment to PIPA (the "Amendment") is intended to update Japan's data protection regime to address the rapid advance in information technology, the rise of the Digital Economy, and the massive increase in global data transfers. The Amendment is the first material change to PIPA since it was originally enacted in 2003.

The Amendment introduces three changes to existing law of particular importance to U.S. multinational employers with employees in Japan. First, the Amendment abolishes the exemption for small businesses. Second, it introduces a new sub-category of "personal information," referred to as "sensitive personal information," that is subject to certain heightened data handling requirements. Third, the Amendment establishes new rules governing the transfer of personal information outside of Japan. In addition, the Amendment establishes a new, independent, regulatory authority, the Personal Information Protection Commission ("PPC"), which replaces the previous supervising authority.[2]

---

1 *See* Philip L. Gordon, "Ten Steps for U.S. Multinational Employers Towards Compliance with Europe's New Data Protection Regime — The General Data Protection Regulation" (Jan. 21, 2016), *available at* https://www.littler.com/publication-press/publication/ten-steps-us-multinational-employers-towards-compliance-europe%e2%80%99s-new.

2 https://www.ppc.go.jp/en/

1. The Amendment Abolishes the Exemption for Small Businesses

Japan's PIPA regulates the collection, transfer, and processing of personal information. The Act broadly defines personal information to include any information about a natural person that can be used to identify that specific individual, including, for example, the individual's name, date of birth, passport number or any other descriptive information.[3]

Under prior law, businesses that handled 5,000 items or less of personal information were excluded from PIPA's privacy requirements. This meant that some smaller Japanese subsidiaries of U.S. multinational corporations, particularly those involved exclusively in business-to-business commerce, were not required to comply with PIPA. The Amendment, however, eliminated this exemption. As a result, all businesses that collect personal information, regardless of the number of items collected, are required to comply with PIPA.

This change is important for employers because employers regularly collect personal information about their employees in order to administer the employment relationship and provide the necessary benefits, compensation, or other entitlements of employment. By eliminating the 5,000-item threshold for coverage, the Amendment extends PIPA's coverage to even small employers within Japan.

2. The Amendment Establishes A New Category Of "Sensitive Personal Information" With Heightened Compliance Requirements

The Amendment creates a new, sub-category of personal information, referred to as "sensitive personal information," and establishes corresponding compliance requirements. Sensitive personal information is defined to include personal information that "require[s] special consideration in handling so as to avoid any unfair discrimination, prejudice or other disadvantage to an individual based on . . . race, creed, social status, medical history, [and] criminal records".[4] This definition encompasses information that employers may collect from job applicants, for example, through pre-employment medical exams and background checks, and from employees, for example, through diversity initiatives, fitness-for-duty tests and sick leave requests.

Under the Amendment, employers generally are required to obtain consent from employees before collecting their sensitive personal information subject to limited exceptions. As relevant to the employment context, consent is not required when collection of sensitive personal information is required by law — as might be the case, for example, when documenting a workplace injury. Consent also is not required when the sensitive personal information is needed to protect health or safety, for example, in the case of a medical emergency.[5]

Under prior law and under the Amendment, employers are required to provide employees with notice of the purposes for which they will use employees' personal information. This notice would have to include the purposes for using any sensitive personal information that the employer might collect. The notice, therefore, provides a convenient opportunity to obtain employees' consent to the collection of sensitive personal information. In addition, employers in Japan should now consider obtaining consent from applicants before running a criminal history background check because criminal records are included within the definition of sensitive personal information.

One key difference in the treatment of sensitive personal information versus personal information is that personal information may be disclosed to a non-agent, third party (*i.e.,* a third party that is not a service provider) through an 'opt-out' scheme. This means that personal information can be disclosed to a third

3 *See* Article 2 of PIPA

4 *See* Article 2, §3 of PIPA

5 *See* Article 17-2 of PIPA

party without the prior express consent of the individual as long as the individual is notified that personal information might be disclosed to the third party. The individual has the right to stop (or opt out of) the disclosure upon request and a notification to the regulator, among other things. This opt-out provision does not apply to sensitive personal information, however. An employer must obtain prior, opt-in consent to the disclosure of sensitive personal information to a non-agent, third party except in the few specific situations referenced above.

3. The Amendment Establishes New Cross-Border Data Transfer Rules

Like many countries outside the United States, Japan now regulates the transfer of personal information to a third country. The Amendment establishes a general rule that the subject of the personal information must consent to the cross-border data transfer. The consent must specifically indicate that the personal information will be transferred to an entity outside of Japan. As with obtaining consent for the collection and disclosure of sensitive personal information, employers can use the mandatory notice regarding the purpose of use as a vehicle for obtaining employees' consent to cross-border data transfers.

The Amendment establishes three circumstances in which consent for cross-border transfers is not required. These circumstances include the following:

a. the receiving party is in a country which has been recognized by the PPC to have standards for the protection of personal information equivalent to those required by PIPA;[6]

b. the transferring party and receiving party have ensured that the receiving party will handle the personal information appropriately and reasonably based on the intent of the provisions under Chapter IV, Section 1 of new PIPA (i.e., executing a data transfer agreement similar to the Standard Contractual Clauses approved by the European Commission for transfers of personal data outside the EU);[7] or

c. the receiving party has a certification recognized by the PPC based on an international framework for handling personal information, such as a certification from the Asia-Pacific Economic Cooperation (APEC) forum's Cross-Border Privacy Rules (CPBR) system.[8]

For U.S. multinational employers, these exceptions likely will not eliminate the need to obtain employees' consent. The transfer of employees' personal data from a Japanese subsidiary to the U.S. parent corporation or a U.S. affiliate would be a disclosure of personal information to a non-agent, third party, putting aside the fact that the personal information is being transferred outside of Japan. Consequently, as explained above, the employee would have to consent to the disclosure.[9]

4. Enforcement by the PPC

The Amendment establishes a new, independent, regulatory authority, the PPC, to oversee implementation of, and enforce compliance with, PIPA. Previously, the ministry responsible for each economic sector or industry had authority to enforce PIPA. This arrangement made it difficult to ensure uniform enforcement. The PPC now exercises its power independently from other administrative bodies and provides guidance and advice, conducts on-site inspections, offers recommendations, and addresses violations of PIPA.

Employers contacted by the PPC for an on-site inspection, or that are subject to compliance recommendations or an order to take steps to mediate alleged violations of PIPA, generally should endeavor to cooperate with the Commission to reduce the risk of criminal prosecution and administrative penalties.

---

6 *See* Article 24 of PIPA (The country covered by this provision has not been specified yet).

7 *See* Article 24 of PIPA and Article11-1 of Enforcement Rules of PIPA

8 *See* Article 24 of PIPA and Article11-2 and Enforcement Rules of PIPA

9 *See* Article 24 of PIPA

PIPA authorizes, in certain circumstances, criminal fines of up to 500,000 yen or one year imprisonment and civil penalties of up to 100,000 yen.[10]

Recommendations

In light of the Amendment, U.S. multinational employers with employees in Japan should consider taking the following steps:

1. Update existing data privacy policies and procedures as may be necessary to comply with the Amendment or implement policies and procedures if none have been implemented to date;
2. Audit the company's practices for collecting, processing, and transferring employees' and applicants' personal information, including sensitive personal information, to ensure compliance with PIPA;
3. Obtain consent of current employees and of new hires to (a) the collection of sensitive personal information, if any; (b) the disclosure of personal information to a non-agent third party; and (c) the cross-border transfer of personal information.

10 *See* Articles 83, 84, 85, and 88 of PIPA