CLIENT ALERTS & INSIGHTS

Amended Japanese Privacy Law Creates New Categories of Regulated Personal Information and Cross-Border Transfer Requirements

MARCH 14, 2022

Authors: Ryan T. Sulkin

The amended law comes into effect in April and covers new categories of personal information, including personal-related information and sensitive personal information.

In June 2021, Japan enacted an amendment to its privacy and data protection law, the Act on the Protection of Personal Information ("**APPI**"). The APPI's new requirements and obligations take effect next month-April 2022-and businesses operating in Japan, or that handle personal information from or located in Japan, should review and update their privacy policies and procedures to ensure they comply with the changes.

The APPI originally passed in 2003, making it one of the early omnibus privacy and data protection laws to be enacted. Since 2003, the law has been amended a number of times, bringing it up to speed with current trends in privacy law and placing more restrictions on businesses, while granting more rights to consumers.

This most recent amendment to the APPI largely focused on further regulating cross-border data transfers (requiring opt-in consent) by creating new categories of information that are regulated under the law (such as personal-related information).

Below is a summary of the key changes that businesses should be aware of.

APPI Scope

To understand the impact of the new amendments to the APPI, it is important to understand the full scope of the law itself.

A business does not need to directly operate in Japan to fall within the scope of the APPI. Instead, the APPI, applies to and regulates the privacy and data protection activities of any business that is considered a personal information handling business operator. Further, a "personal information handling business operator" includes any business that provides a personal information database for commercial use. Under the APPI, a "personal information database" essentially includes any assembly of personal information that is arranged in a way so that specific personal information can be retrieved via a computer.

Generally, any business that receives or collects Japanese personal information in connection with providing services or products to individuals located in Japan, the business will be subject to the APPI, whether or not the business itself is located in Japan.

Subsequently, “personal information” under the APPI includes any information that can (i) identify an individual; or (ii) contains an “Individual Identification Code.” This second category of personal information includes computer-generated numbers, symbols, or code that are used to identify a body feature and to identify an individual person (i.e., fingerprint scanning); or a number, symbol, or other unique identifier assigned to a service or product provided to an individual so as to identify that individual.

While the scope of the APPI is narrower than other omnibus privacy and data protection laws (such as the EU’s General Data Protection Regulation), the APPI is still generally applicable to consumer-facing businesses operating in Japan.

Cross Border Data Transfer

One of the biggest shifts under the APPI amendments are the new requirements placed on businesses that transfer personal information from Japan to another location.

Beginning April 2022, businesses within the scope of the APPI will need to either (i) obtain an individual’s opt-in consent prior to transferring that individual’s personal information to a location outside of Japan; or (ii) establish a personal information protection system with the party receiving the personal in the foreign jurisdiction.

For the opt-in consent to be effective and operative, the individual must-at the time they consent to the transfer-be informed about the privacy and data protection laws set forth in the country the personal information is being transferred to, the safeguards and measures the business has implemented and maintained to ensure the protection of the personal information, and any other information deemed necessary by Japan’s Personal Information Protection Commission in any application regulation or guidance.

Further, if the personal information that is subject to a cross-border transfer is also transferred to a third party in that foreign country, the business must ensure that the third party complies with the safeguards and measures that the business set forth in its notice to the individual.

Under the personal information protection system option, a business transferring personal information from Japan to another country needs to execute a contract with the foreign country party receiving the personal information. For example, if transferring personal information to the U.S. and to a U.S.-based third party processor, a business would need to implement contractual guarantees that the third-party is complying the requisite safeguards. The safeguards that must be included in such a contract must set forth “necessary measures” to obligate the receiving party to handle the personal information in accordance with the APPI.

Sensitive Information

The amended APPI also introduces new categories of regulated information; one of which is sensitive personal information, which is referred to as “special care-required personal information.”

Under the APPI, sensitive personal information includes any information about an individual’s race, creed, social status, medical history, criminal records, crime victim’s history, or any other information that may lead to social discrimination or disadvantage. The definition of sensitive personal information under the APPI focuses heavily on social and ethnic information that could lead

to discrimination. This is a narrower definition than provided under other omnibus privacy and data protection laws, which also include such information but also include financial information, biometric information, and/or location information.

Businesses within the scope of the APPI cannot collect or use an individual's sensitive personal information without first obtaining their prior, opt-in consent.

Personal Related Information

A second new category of information the amended APPI adds is personal-related information. "Personal related information" includes any information that is related to an individual that does not fall within the scope of personal information, pseudonymous information, or anonymous information.

What differentiates personal-related information and information that is wholly outside the scope of the APPI is that personal-related information could still be used to identify an individual if connected to further information. While there are no specific examples in the APPI, cookies and IP addresses would likely fall within this category.

Similar to personal information, no opt-in consent is required before a business collects personal related information. Instead, notice and choice, in the form of a privacy policy that properly accounts for the purposes the personal related information is collected, is sufficient.

Pseudonymous Information

Another new concept the amended APPI contemplates (in line with most other omnibus privacy and data protection regulation), is pseudonymous information. Such a category of information was not originally considered under the APPI.

Pseudonymous information under the amended APPI includes information that relates to an individual but that is processed in a manner that does not identify a specific individual unless connected to other information that could identify the individual Therefore, otherwise pseudonymous information is considered personal information if it is connected to identifying information (i.e., stored with personal information).

Specifically, the amended APPI sets forth the only methods that otherwise personal information can fall into the pseudonymous information category. There are three methods: (i) by deleting all descriptions or information identifiable to a specific individual; (ii) by deleting all personal identification numbers; or (iii) by deleting all descriptions that would cause economic damage if breached.

The amended APPI's definition of pseudonymous information is broader than other concepts frequently used in omnibus privacy and data protection laws, such as anonymized information or de-identified information.

Data Breach Notification

As originally drafted, and as drafted in its most recent iteration, the APPI did not require mandatory data breach notifications to the Personal Information Protection Commission.

However, under the newly amended APPI, businesses within the scope of the law must report a data breach to the Personal Information Protection Commission if the breach includes: (i) sensitive

information; (ii) data that could result in significant economic loss (i.e., financial information); (iii) an "unjust purpose," such as personal information hijacked by ransomware; or (iv) more than 1,000 individuals' personal information.

A business must "promptly" provide the initial notification to the Personal Information Protection Commission. Additionally, a second and final notification is required within 60 days if the breach involved more than 1,000 individuals' personal information, or 30 days if the breach falls within any of the other three categories listed above.

The final notification must inform the Personal Information Protection Information Commission of a summary of the incident, categories of personal information involved, the total number of individuals affected, the root cause, extent of damage (including any indirect damage that could result), and any actions taken since the data breach occurred.

While penalties and fines under the current APPI are smaller than those provided under other omnibus privacy and data protection laws, the amended APPI implements new penalties and fines on business if an employee fraudulently leaks or uses personal information. The fine that can be levied against a business for such a violation tops out at $930,000, with additional fines possible against the actual individual who committed the fraudulent act.

Takeaways

Businesses that operate in Japan or that handle personal information originating in Japan should be reviewing-and making any required updates to-their privacy policies and procedures. This review and update process should be completed prior to April 2022.

As the Japanese privacy regulatory structure continues to develop and the obligations your business is required to take on grow, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.