

New Amendments Passed to Japan's Data Privacy Law

Article By:

Scott A. Warren

Maika Kawaguchi

In the midst of revising the Japan Civil Code and the foreign attorney laws, Japan has recently passed amendments to its data privacy law, the [Act on the Protection of Personal Information](#) ("APPI"). Some of these changes put Japan's law closer in line with the EU's General Data Protection Regulation "GDPR" as to which both have recognized the adequacy of each other's data privacy regimes. As a result, transfers of personal information from Japan to all third countries will be subject to stricter controls when the amendments become fully enforceable, which is expected to occur in 2022.

The main changes to the APPI relate to the following:

Expanding Individual Rights: There are provisions expanding an individual's rights to require the deletion or disclosure of personal information ('PI')

- where there is a possibility of violating the data subject's rights or legitimate interests;
- in the event of a breach of the APPI via transfer to a 3rd party;
- to include short-term data which is kept for 6 months or less; and
- allowing the data subject to request the format of the disclosure of their data, including in a digital format.

Personal information, other than sensitive data, could be transferred to 3rd parties without express consent as long as notice of the transfer was publically disclosed and there was no objection by the data subject (essentially an opt-out provision). Under the old law, personal information transferred to a 3rd party on an opt-out basis could be re-transferred by the 3rd party to another party on a similar opt-out basis. However, under the new Amendment, if the personal information has already been transferred to a 3rd party on an opt-out basis, the further transfer on that basis is not allowed. For further transfer, either direct consent or one of the other legal transfer grounds must be in place.

Importantly, please note that under the APPI, the law does not distinguish between 'Controller' and

‘Processor’. Accordingly, if the entity collecting/using the data has another entity process the data on its behalf (with no other purpose) and under proper contract, it is not considered a transfer under the law. 3rd party transfers occur when the data is transferred to another entity to use the data for other purposes.

Breach Notification: Under the new Amendment, companies are required to notify the individual and data privacy authority (Personal Information Protection Commission (‘PPC’)) in the event an incident falls under certain designated criteria as potentially causing the violation of individual rights and interests. The report to the PPC will consist of providing a preliminary report ‘as soon as possible’ to state the situation, followed by a more detailed report as to the causes and remedial measures implemented. The timing for the submission of the more detailed report is still to be determined. If giving a notice to the individual is difficult, it could be replaced with a public announcement of the incident and setting up of an inquiry desk.

Encouraging Private PI Protection Organizations: The Amendment has provisions designed to expand the number of accredited organizations providing PI protection advice to organizations, such as providing Japan Privacy Mark, CBPR and other privacy certifications, or setting up self-regulatory guidelines that fit to certain businesses or industry.

Creating New Concepts in PI Utilization: the new Amendment recognizes ‘pseudonymization’ and, when properly implemented, it eases disclosure and cessation requirements on an organization. It further confirms the need to obtain consent for the transfer of pseudonymized data to a 3rd party if that data is expected to become personal information once in the hands of the 3rd party. For example, if the transferring party provides non-identifiable data to an entity that is able to add elements that would make it PI, then the data subject’s consent for the transfer must be obtained.

Substantially Increases Penalties: For organizations, penalties for violation of the law have been increased up to ¥100M (around US\$1M). Individual violation of a PPC order is punishable by up to 1 year imprisonment or a fine of up to ¥1M (@ \$10k). The false submission of reports may be fined up to ¥500k (@\$5k).

Cross-Border Application: The Amendment clarifies that its provisions, obligations and penalties apply to entities outside of Japan that supply goods or services in Japan and handle PI from an individual in Japan. In essence, this does not change Japan-US data flows, for example, other than the amendments indicated above. But it does make it clear that entities outside of Japan are subject to the law.

Although the above changes have been decided, not all of the details concerning enforcement are yet determined. The Cabinet Order and Commission Rules are expected to be issued for public comment by the end of this year, with the Implementing Guidelines expected for public comment anticipated by the middle of 2021. The full implementation of the Amendment is planned for the Spring of 2022.

© Copyright 2025 Squire Patton Boggs (US) LLP

National Law Review, Volume X, Number 232

Source URL: <https://natlawreview.com/article/new-amendments-passed-to-japan-s-data-privacy-law>