Skadden

September 2018

# Data Protection in Japan to Align With GDPR

On July 17, 2018, less than two months after the General Data Protection Regulation (GDPR) went into effect, Japan and the European Union agreed to recognize each other's data protection regimes as providing adequate protections for personal data. The European Commission said in a press release that the move will create "the world's largest area of safe data flows." Once finalized, these "reciprocal adequacy" decisions will allow personal data to flow between companies in Japan and the EU without being subjected to additional safety checks. From a European perspective, Japan will be recognized as having "adequate safeguards" in place for data protection, meaning that specific transfer agreements with Japanese entities may no longer be required.

Even though the EU already has unilateral adequacy decisions with several other countries, this is the first time the EU and a third country have agreed on a reciprocal recognition of the adequate level of data protection. Other countries may follow suit and similarly obtain reciprocity.

The mutual adequacy finding will complement the existing trade benefits of the Japan-EU Economic Partnership Agreement and contribute to the Japan-EU strategic partnership by facilitating the data flow between them. Companies are expected to benefit from unhindered, safe and free data transfers between the two economies that would remain restricted in the absence of the reciprocity recognition.

## Processing Personal Data Transfers From EU to Japan

The European Commission is expected to formally adopt its adequacy decision on Japan this fall. After Japan is whitelisted, personal data transferred from companies in the EU will be deemed to be protected by the same standards as in the EU if processed in accordance with Japanese law. To achieve this, Japan agreed to implement additional safeguards to align with the EU's standards. Specifically, Japan agreed to put in place stricter guidelines for the re-transfer of personal data that originally was transferred from within the EU to a company in a third country and additional limitations on the use of sensitive data. Japan also agreed to implement a new mechanism to allow EU residents to file complaints with Japan's data protection authority if public authorities in Japan unlawfully access their data.

On September 7, 2018, Japan's Personal Information Protection Commission (PPC) announced supplementary rules regarding how personal data transferred from the EU should be processed following the adequacy recognition. The rules will come into effect when the European Commission formally adopts that Japan has secured adequate level of protection for personal data pursuant to Article 45 of the GDPR. According to the rules, five major substantive changes will be implemented with respect to the current Japanese regulations, as summarized in the chart

below. These changes are intended to tighten data privacy regulations in Japan to align with the GDPR. The rules will apply only to personal data transferred from the EU under the adequacy recognition.

| Items to Be Aligned | Current Law in Japan | PPC's Supplementary Rules | Practical Implications |
|---|---|---|---|
| Scope of "personal information requiring careful consideration" | Information regarding data subjects' sex lives, sexual orientation and labor union memberships is not considered "personal information requiring careful consideration" | Information regarding EU data subjects' sex lives, sexual orientation and labor union memberships is to be treated as "personal information requiring careful consideration," to align with "sensitive personal data" as defined under the GDPR | Consent of EU data subjects would be required to acquire such information. Provision of such data to a third party by way of an opt-out arrangement would be prohibited (*i.e.*, express consent would be required) in accordance with Japanese laws |
| Access right | Data subjects do not have a right to access their personal data if it is to be deleted within six months. They have access rights to personal data that is not to be deleted within six months. | Companies will be obligated to disclose personal data held by them upon the EU data subject's request, regardless of the duration for which such data will be held | Companies that collect personal data from EU residents and retain that data for any period of time will need to comply with requests for disclosure from data subjects |
| Succession of purpose of use | No specific rules | Personal data of EU data subjects received from a third party is to only be used in accordance with the purpose for which it was originally collected | Companies will need to confirm and track the purposes for which personal data of EU residents was originally collected and limit their use of such personal data accordingly. Proper tracking of permitted uses of different data sets may be challenging and may require new technologies or processes with attendant |

| | | | |
|---|---|---|---|
| | | | costs. |
| Re-transfer of EU data subjects' personal data from Japan to foreign countries | Allowed when:<br>(i) consent of the data subjects is obtained;<br>(ii) adequate steps to protect the security of the data are taken between the transferor and the transferee; or<br>(iii) the transferee is located in a foreign country designated by the PPC | Points (i) and (iii) continue to hold. Regarding point (ii), protection equivalent to that under Japanese law must be secured as between the transferor and the transferee, either by contract or (if the transferee is a group company) the group company's internal rules. | The current Japanese law is unclear on point (ii), but the supplementary rules will clarify that a contract with a third-party transferee is required unless consent of the EU data subject is obtained or the transferee is located in a whitelist country designated by the PPC |
| Anonymously processed information (that is exempt from certain protections) | Certain data may be treated as "anonymously processed information" even if the information necessary to identify the data subjects is kept separately (*i.e.*, the data is readily susceptible to de-anonymization) | In order to be treated as "anonymously processed information," information regarding the method for anonymization process must be deleted | To be exempt under Japanese law, companies will need to make sure that information on anonymization process is deleted (as opposed to simply separated from the data) |

**Other Differences Between Japan's Data Privacy Law and GDPR**

Entities operating in Japan must comply with its Act on Protection of Personal Information (APPI), whether or not cross-border data transfers occur. APPI is different from the GDPR in several respects; the material differences are highlighted in the chart below. Generally, the GDPR provides greater protection for data subjects and stricter regulations on the companies that process personal data than the APPI.

| | APPI | GDPR |
|---|---|---|
| Sensitive data | Prior consent required for acquiring and disclosing sensitive data | Processing is generally prohibited |
| Data portability right | Data subjects only have the general right to request a copy of their personal data | Data subjects have the right to receive their personal data in a structured, commonly used and machine-readable format and have the right to transmit such data to another |

| | | |
|---|---|---|
| | | controller |
| Obligation to record data processing activities | Applicable only when personal data is provided to a third party (in which case the date, the recipient's identity and other background information must be recorded by the transferor) | Applicable to all processing including, but not limited to, disclosure to a third party |
| Obligation to report to supervisory authorities in case of data leakage | Obligation to make an effort to report; no specific time limit | If breach is likely to present a risk to data subjects, obligation to notify authorities without undue delay, and within 72 hours if feasible, after becoming aware of the breach |
| Data protection officer | Appointment not mandatory, although obligations to oversee employees and to implement safety control measures exist | Appointment mandatory in the following cases:<br>- when regular and systematic large-scale monitoring of data subjects is required; or<br>- when processing certain sensitive data on a large scale |

The PPC supplementary rules will not address these differences, as that would be beyond the intended scope. These gaps may only be filled through an amendment to the APPI. That being said, given that the APPI underwent major and thorough revisions that took effect in 2017, it is uncertain whether another fundamental revision to the APPI would be implemented anytime soon. Therefore, for entities operating in Japan, it is important to grasp the differences between the APPI and the GDPR, which has become the global standard.

**Practical Implications and Considerations**

Today, some companies that transfer personal data from the EU to Japan do so pursuant to standard contractual clauses (SCCs) published by the European Commission. Japanese companies using SCCs might assume that they can readily terminate these agreements once the adequacy decision is formally adopted. However, companies should keep in mind that the adequacy decision only applies to EU-Japan transfers, and SCCs between the EU and other jurisdictions will need to remain in place. Companies should also keep in mind that the EU is likely to issue an updated version of the SCCs that complies with GDPR requirements and replaces current SCCs.

**Discussions Between Japan and Other Nations**

In order to ensure the mutual and smooth transfer of personal data between companies in Japan

and the U.S., PPC is in discussions with the U.S. Department of Commerce to promote cooperative relationships for the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules system, a multilateral arrangement to certify compliance with the APEC Privacy Framework. PPC is seeking to promote the participation of other Asian countries as well as domestic enterprises, with an aim to interoperate with the EU's personal data transfer regime.

The Japanese government also is in discussions with certain U.K. authorities, including the Department of Digital, Culture, Media and Sport, and the Information Commissioner's Office, for a personal data transfer agreement that would ensure smooth transfer of data between companies in those two countries as well.