

Data Privacy Laws and Regulations in Japan - Part 1

APPI 2017 and recent amendments

28 April 2021

Speakers



Hiroto Imai

Partner
Tokyo



Mizue Kakiuchi

Associate
Tokyo



Eva-Marie Koenig

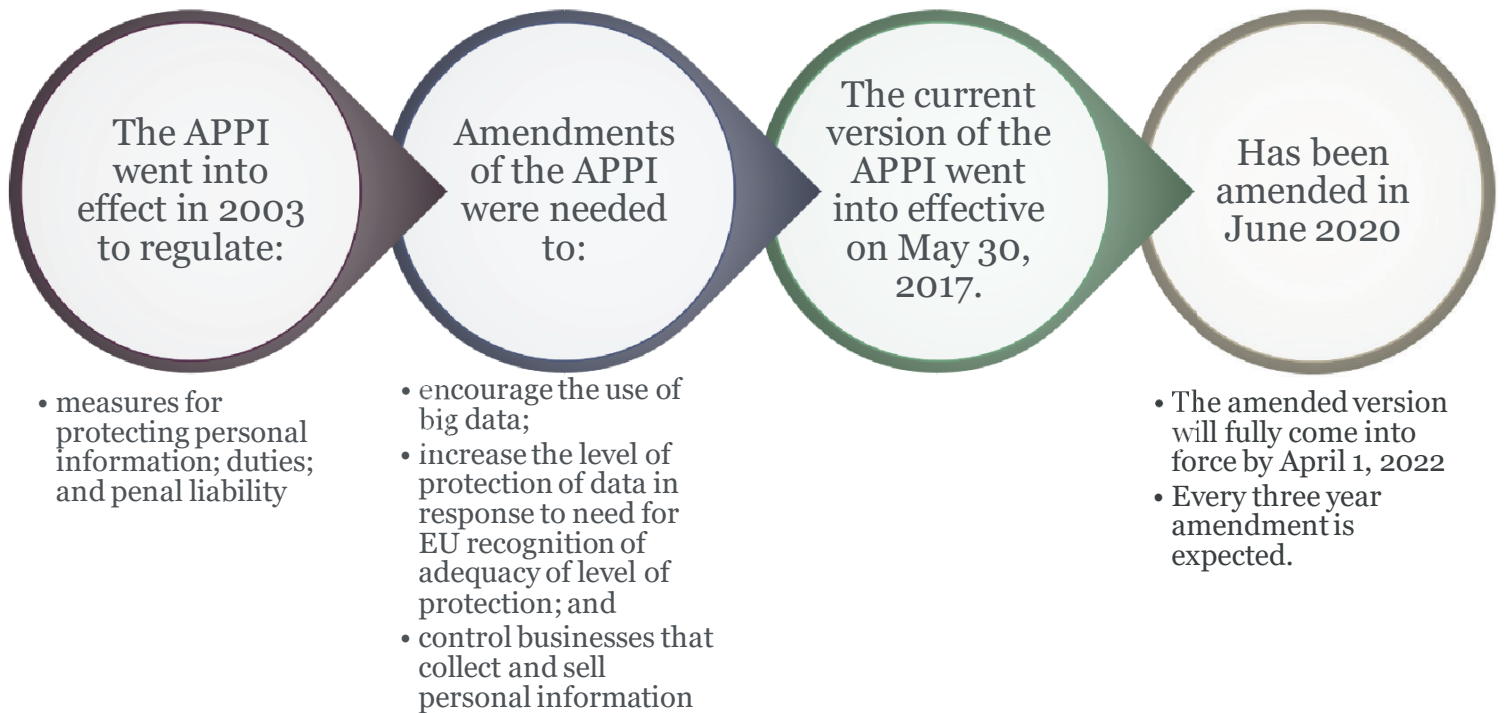
Associate
Tokyo



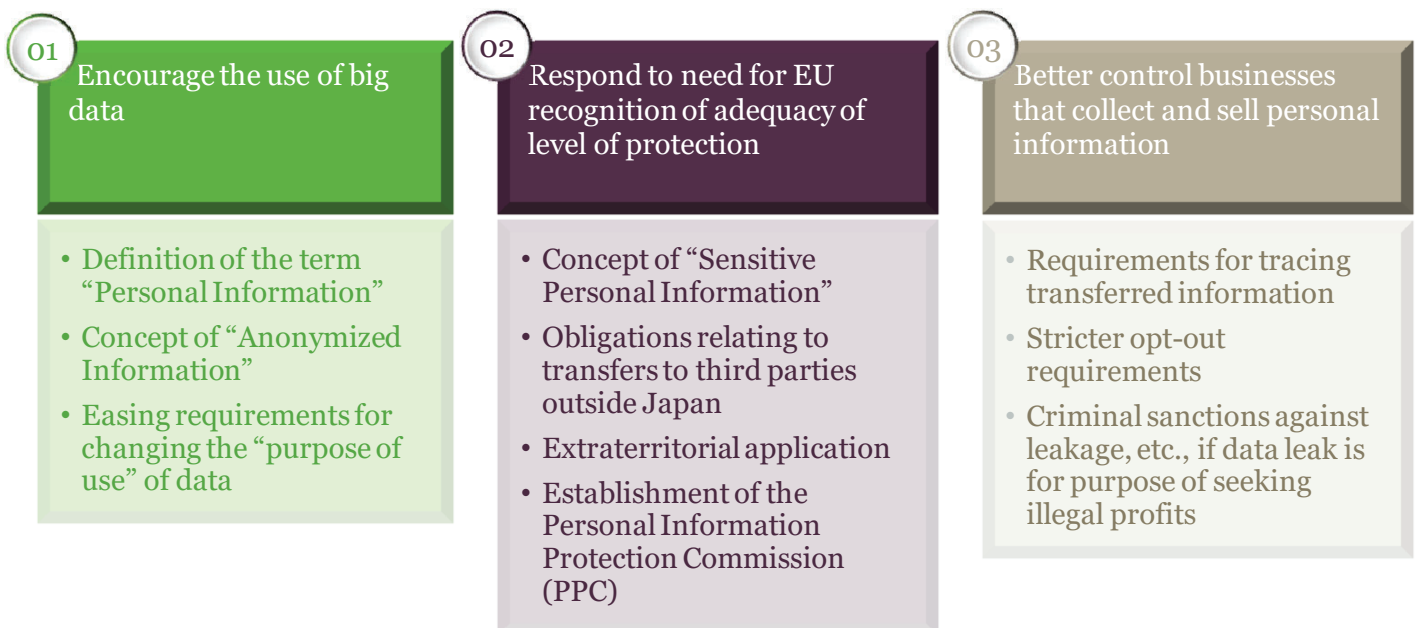
Japan

Act on the Protection of
Personal Information

The Act on the Protection of Personal Information (APPI)



Goals of the current APPI



Definition of Personal Information

APPI: ARTICLE 2(1)



Information about a living individual



Includes information that can be cross-checked for identification

(e.g., name, DOB, biometric data, genetic data, personal identification numbers)

Personal Data is Personal Information contained in a database (whether electronic or not) that enables easy retrieval

GDPR: ARTICLE 4(1)



Location data¹, online identifier², economic, cultural, and social data



NA

¹ Included in the APPI, not explicitly stated

² IP address, online handle, etc.

Anonymized Information – Article 2(9) and 36

- Any Personal Information about a Data Subject that has been sufficiently processed so that any information that could identify a specific Data Subject has been removed and cannot be restored
- Once anonymized, the Data Subject's Personal Information **must not be restored to a state where they can be identified**
- If information is anonymized properly (and other relevant rules are complied with), it is not considered Personal Information
- However, when producing anonymized data to a third-party, the Data Handler must still disclose the categories of information provided to the third party as well as the method of providing the information

Anonymized and Pseudonymized Information

APPI: ARTICLE 2(9)



Personal information that has been sufficiently processed



Sufficiently processed means that identifying traits of the data have been removed and cannot be restored



Once anonymized, must not be restored to a state where Data Subject can be identified

GDPR: ARTICLE 4(5)



NA



Does not explicitly state that the data cannot return to its pre-pseudonymised state

Note: anonymization and “pseudonymisation” are different

Special care required information – Article 2 (3)

- Specific category of Personal Information
- Definition: information relating to race, religion, medical history, and other personal information having the potential to lead to unjustified discrimination or prejudice
- In principle, **prior consent** of the Data Subject is required to **obtain** (NOT merely use) special care required information
- Opt-out for both obtaining and transmitting special care required information is not possible

Special care required Information

APPI: ARTICLE 2(2-3)

- 01** Individual identification code, race, religion, medical history, social status, criminal record
- 02** Has the potential to lead to unjustified discrimination or prejudice
- 03** Prior consent is required to obtain and use



GDPR: ARTICLE 9 (SENSITIVE DATA)

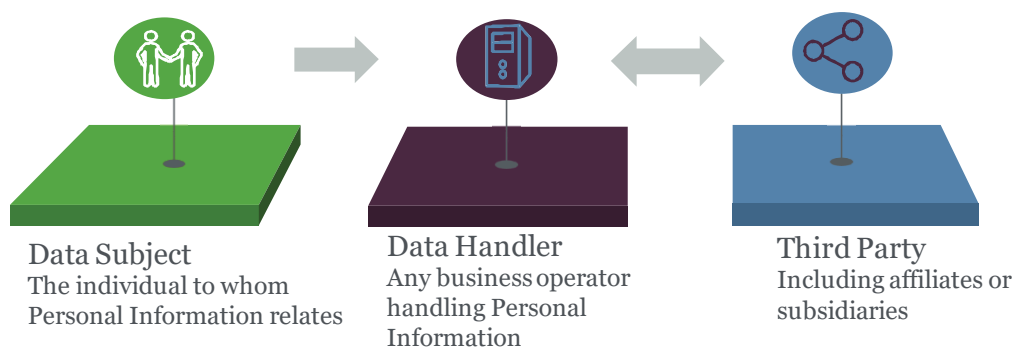
Genetic data 4(13), Biometric data 4(14), data concerning health 4(15), political opinion, philosophical beliefs, trade union membership, or sex life



NA

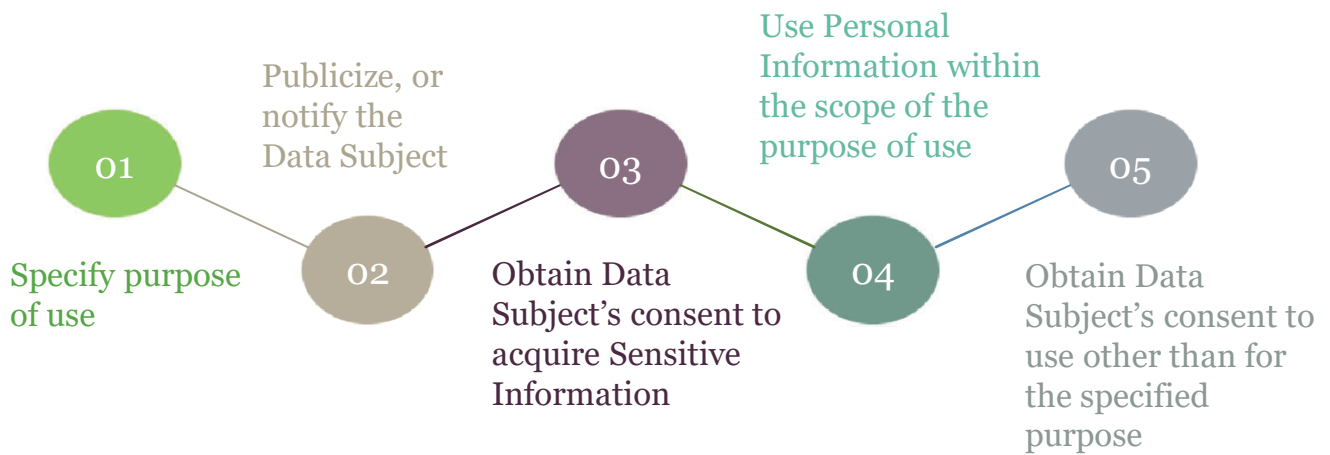
Note: For EU recognition of adequacy of level of protection, the APPI treats sex life, sexual orientation and labor union which is sensitive data under the GDPR as special care required information relating to personal data from EU countries

Parties involved in the transfer of information under APPI

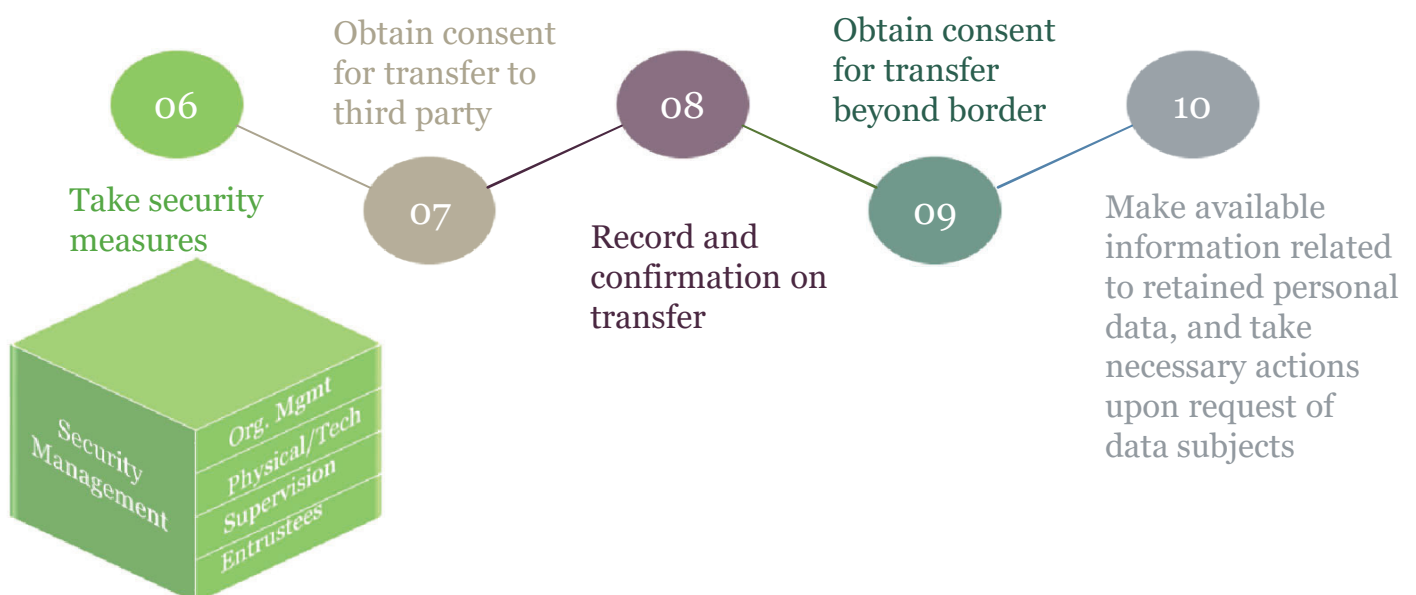


Note: GDPR's "controller" and "processor" are both considered "Data Handlers" under the APPI

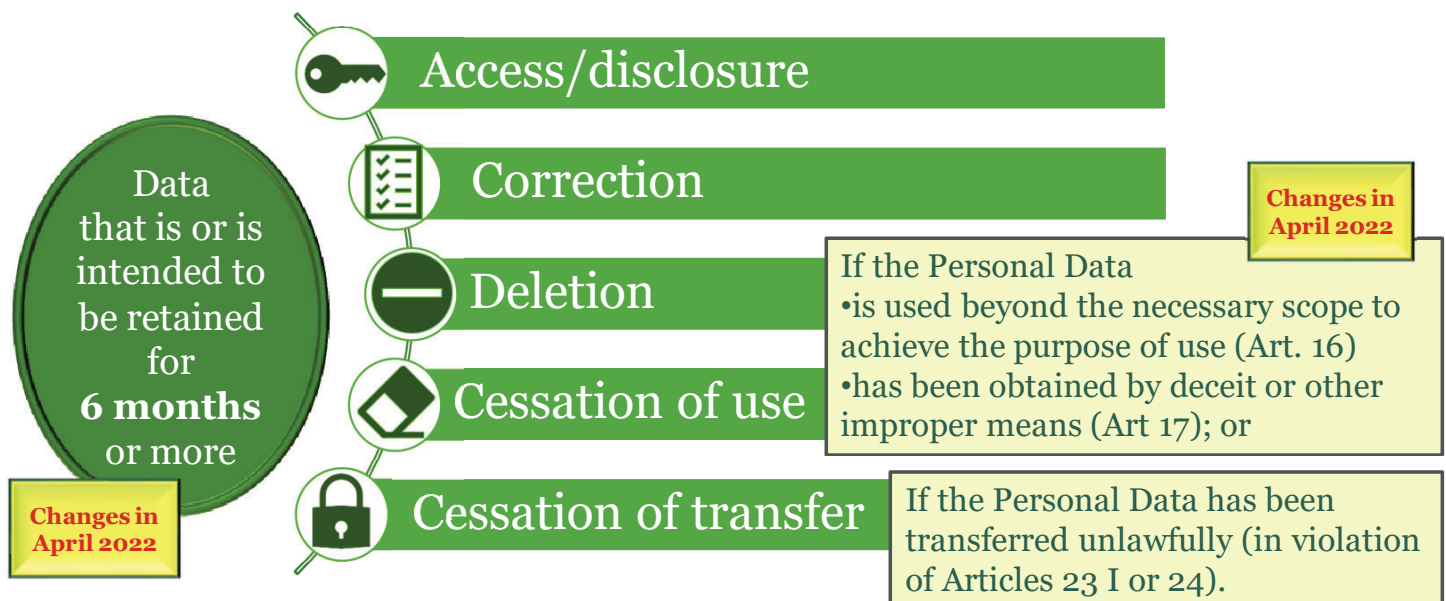
Basic Obligations if Personal Information is obtained



Basic Obligations for handling Personal Information



Rights of Data Subjects under the current APPI



Utilization Cease

APPI: ARTICLE 30(1), (3)

- 01 May demand **utilization cease** or **deletion** if APPI Article 16 or 17 is violated
- 02 May **demand cease of third-party provisions** if APPI Article 23(1) or 24 is violated

Changes in April 2022: Data Subjects may demand utilization cease, deletion, or cease of transfer in additional cases.

GDPR: ARTICLE 17-18, 20-21


- “Right to be forgotten” (Art. 17)
 - Right to restrict the processing (Art. 18)
 - Right to data portability (Art. 20)
 - Right to object (Art. 21)
- NA

Disclosure of data to a Third Party – (Article 23)

- In principle, the prior consent of the Data Subject must be obtained unless the disclosure is:
 - based on laws and regulations;
 - to protect human life, safety, health and properties (and difficult to get a consent);
 - to protect public hygiene or promote fostering children (and difficult to get consent);
 - to cooperate with national or local governments
- Transfer history (name, reason, date, content, etc.) must be recorded and retained

Other exceptions relating to disclosure to a Third Party

- A Data Handler can disclose Personal Data to a Third Party without the prior consent of the Data Subject if the requirements of the **opt-out method** are met
- If the Personal Data is transferred as part of an **entrustment** or **joint use**, or in connection with **business succession**, the transferee will not be considered a Third Party under the APPI
- There are additional requirements for using these exceptions when transferring Personal Data to a Third Party in a foreign country



Since October 2021, this is more restricted.

Obligations relating to **traceability** of Personal Data

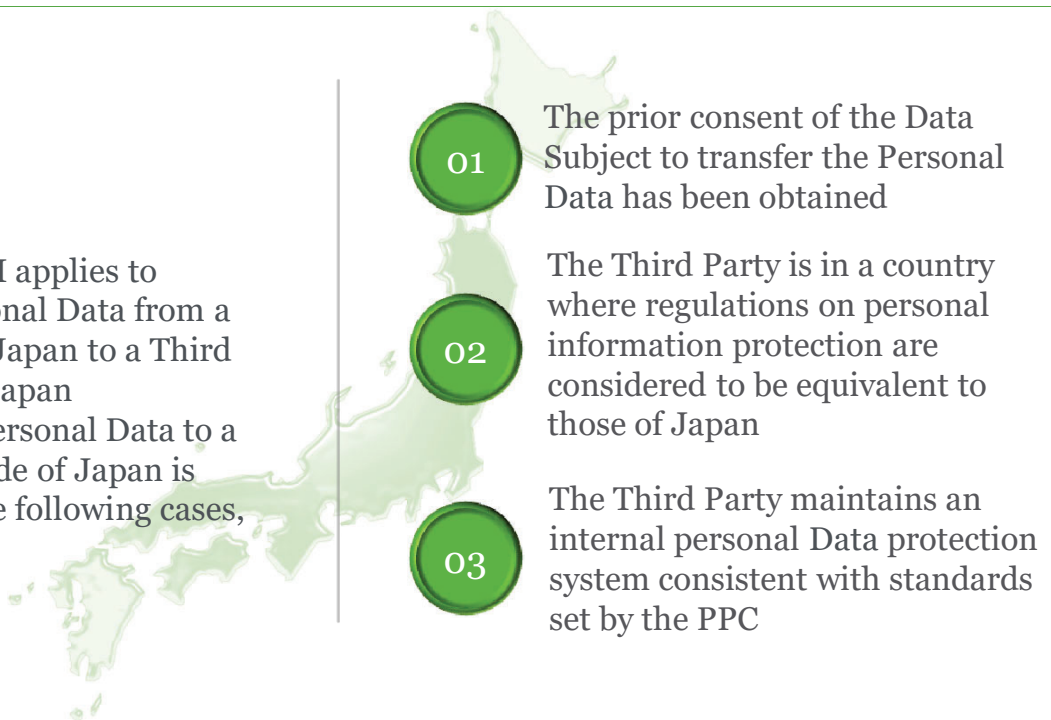


- It must be possible to trace when and by whom Personal Data was provided and received, in order to deter improper use of Personal Data
 - To keep the information traceable, the Data Handler must **record and retain the details of the transfer** at the time of transfer

Transfers to a Third Party in a foreign country

Article 24

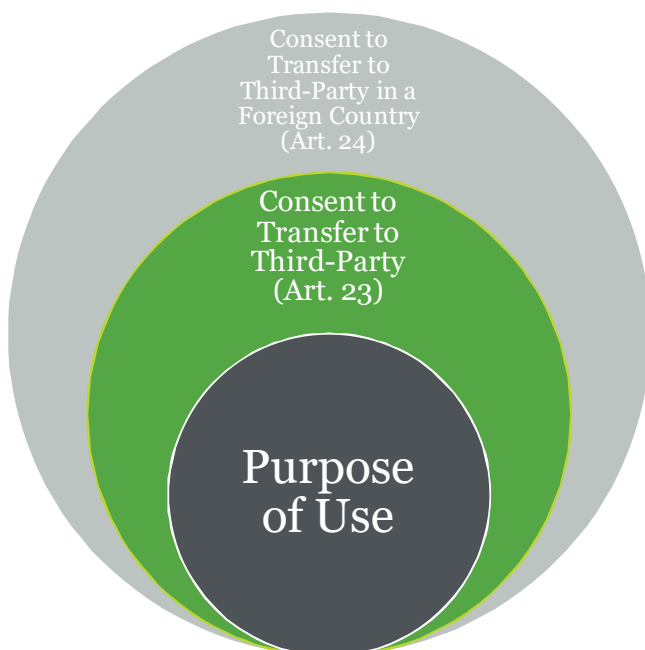
The Current APPI applies to transfers of Personal Data from a Data Handler in Japan to a Third Party outside of Japan
The transfer of Personal Data to a Third Party outside of Japan is permissible in the following cases, for example:



Transfers to a Third Party in a foreign country

- 02 The Third Party is located in a country where regulations on personal information protection are considered to meet the adequate level of protection in Japan
 - EEA
 - UK
- 03 The Third Party maintains an internal personal Data protection system consistent with standards set by the PPC
 - Data Transfer Agreement
 - Internal group policy
 - Certification of CBPR (APEC Cross-Border Privacy Rules)

APPI on transfer to Third-Party & foreign country

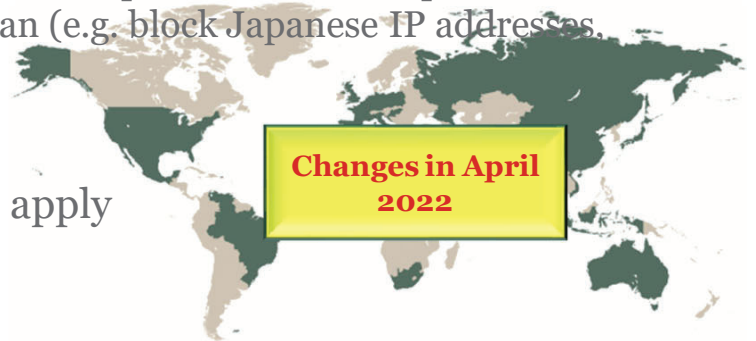


- Can get consent to transfer to a third-party and to a foreign country at once
- It is recommended to specify third-party and country when getting the consent

Changes in April 2022:
Provide **certain information** regarding the protection of such transferred Personal Data **to the Data Subject**

Extraterritorial application of the APPI – Article 75

- If a company operating outside Japan **engages in the supply of a good or service to a person in Japan**, the APPI will apply with respect to Personal Information collected in relation to such good or service in Japan
- The standard to determine whether there is **engagement** in Japan is, for example:
 - Does the foreign company have a system in place sufficient to prevent the provision of goods or services to Japan (e.g. block Japanese IP addresses, refuse shipment to Japan)?
- If not, most of the main requirements of the APPI will apply



Extraterritorial application

APPI: ARTICLE 75



Company operating outside of Japan and engages in activity of the supply of goods or services to an individual within Japan will be subject to the APPI for information collected for activities in Japan



GDPR: ARTICLE 3

Applies to controllers/processors with establishment **in** the EU, regardless of whether the processing takes place in the Union or not, or **outside** of the EU if offering goods/services to data subjects in the EU or monitoring of their behavior in the EU

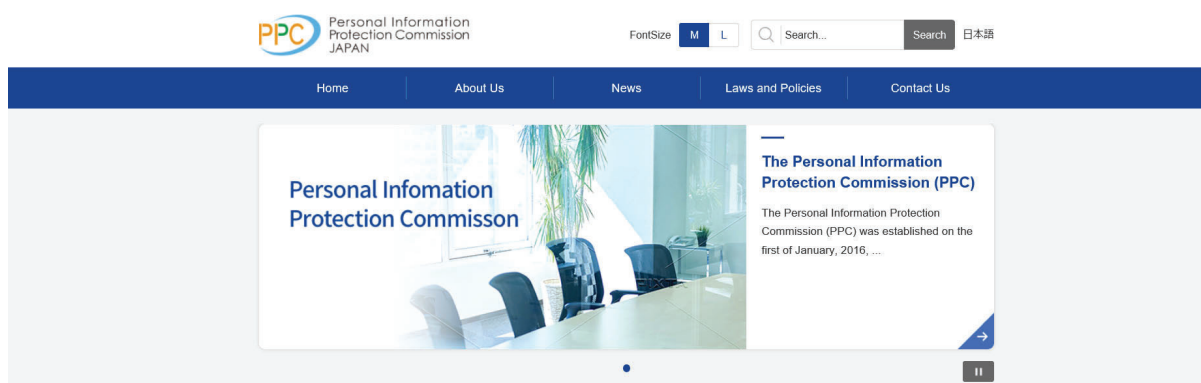
Other features of the APPI (e.g. compared to the CCPA)

- All business operators who handle personal information are covered (e.g. no limitation in scale of business)
- “Purposes of use” should clearly be stated in privacy policy, rather than “how data is used” or “why we use”.
- No periodical revision of privacy policy is required
- No notice is required other than a privacy policy at present
 - Do Not Sell My Personal Information
 - Cookie policy
- Marketing advertisements or emails are not regulated under the APPI, but there are rules in other Acts
- No specific restrictions for Children (Please note that feasibility of consent should be considered under the APPI as well)

Personal Information Protection Commission (PPC)

- Established on January 1, 2016 by the Current APPI
- Independent government body that has the authority to handle matters relating to personal information protection in Japan

<https://www.ppc.go.jp/en/>



The amended APPI will fully come into effect on
1 April 2022.

Is your business ready for the changes?
We're here to help.

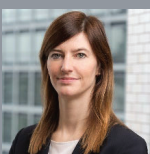
Contacts



Hiroto Imai
Partner, Tokyo
hiroto.imai@hoganlovells.com



Mizue Kakiuchi
Associate, Tokyo
mizue.kakiuchi@hoganlovells.com



Eva-Marie Koenig
Associate, Tokyo
eva-marie.koenig@hoganlovells.com

