

Data Privacy Laws and Regulations in Japan - Part 2

APPI 2017 and recent amendments

28 April 2021

Speakers



Hiroto Imai

Partner
Tokyo



Mizue Kakiuchi

Associate
Tokyo



Eva-Marie Koenig

Associate
Tokyo

A background image showing lines of green code on a dark screen, resembling a computer terminal or a code editor. The code is partially obscured by a dark green overlay box.

Amended APPI

Announced on June 2020
Fully effective by April 1 2022

Amendments 2020

Goals

Respond to the increased need to balance the protection and utilization of personal information with the risks arising from domestic and cross-border data transfers

Note: The APPI is revised every three years.

01

Broaden Data Subjects' powers to exercise control over their data

02

Facilitate corporation's internal use of "big data"

Amendments 2020 – key provisions

1. Expanding rights of Data Subjects
2. Mandatory breach reporting/informing
3. Expanding types of data
4. Restricting exception for third-party transfers
5. Additional obligations for international transfers
6. Strengthening of penalties
7. More effective extraterritorial applicability

1. Expanding rights of Data Subjects



Data Subjects may request that a Data Handler **cease use of, cease provision to a third party**, where there is (i) no reason to use the data anymore, (ii) a serious data breach incident; (iii) a risk of violating individual rights or legitimate interests Art. 30 V



Data Subjects may choose the **method** (in writing or through electronic means such as by email) to receive Personal Data upon exercising the right of **access**. Art. 28



Data Subjects may also request Data Handlers to **disclose records of transfers** of Personal Data to third parties. Art. 28



Data Subjects may request Data Handlers to make **available more information** of its retained Personal Data (e.g. address, representative's name of Data Handler). Art. 27



Broadened scope of retained data which a Data Handler must disclose to a Data Subject upon request **regardless of the retention period**. Art. 2 VII

2. Mandatory breach reporting / informing (1) Art. 22-2

- Where data breaches “likely harm the rights and interests of individuals”, it will be required:
 1. to report to the relevant **authority** in specified time frames and
 2. to inform affected **individuals** timely.

Note: Any involved business operator needs to report in general, but in case of entrustment, if the entrustee reported to the entrustor ASAP, the reporting obligation of the entrustee to the authority may be waived.

2. Mandatory breach reporting / informing (2) Art. 22-2

- Reporting will be required in the following (possible) scenario:

- ① a leakage of **special care required Personal Data** (excluding data with protection measures such as encrypted data)
- ② results in a risk of **property damage**,
- ③ which is based on an **intentional violation** of the law such as unauthorized access, or
- ④ affects at least **1,000 Data Subjects**.



2-1. Mandatory breach reporting – to Authority

- The updated APPI makes it mandatory for Data Handlers to report a data breach to the Authority in Japanese.
 - PPC via its **website**
 - Other authorities (e.g. Telecommunication business, Financial business)
- Timing
 1. **Initial** report
 - Information to the extent possible
 - As soon as possible after breach is found
 - Subsequent reports may be required based on the Authority's instructions
 2. Final report with full details
 - 30 days
 - 60 days in case of intentional breach



2-2. Mandatory breach informing

– to **Individuals**

- The updated APPI makes it mandatory for Data Handlers to inform affected individuals about a data breach
 - This is exempted if it is difficult to inform the individuals, and a substitute measure can be taken to protect the Data Subject's interests
- **No specific timing** set out in the APPI, but “in a timely manner”
- In practice, notice is generally combined with apologies



Note:

- There is a risk of civil actions brought by individuals even if there is no informing obligation
- Sincerity is important in Japan with very carefully chosen legal language and appropriate expression

3. Expanding types of data



Pseudonymously Processed Information



Personal Related Information



Removing the 6 month retention-period exception from the scope of retained Personal Data

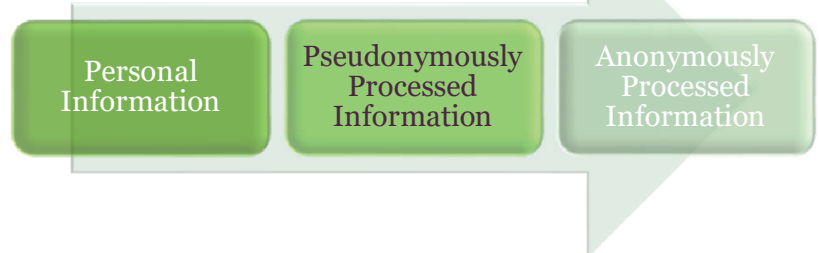
Note:

These new types of data are applicable extraterritorially.

3-1. Pseudonymously Processed Information

Art. 35-2

- The amended APPI introduces the concept of “Pseudonymously Processed Information”. Art 2 IX
- Data Handlers can utilize pseudonymized data in limited circumstances, while obligations of dealing with Data Subjects’ rights such as for disclosure and cease of utilization will be eased
- Differing obligations compared to non-pseudonymized personal data:
 - Limitation to change purposes of use (Art. 15II)
 - Reporting obligation (Art. 22-2)
 - Individuals’ rights (Arts. 27~34)



3-2. Personal Related Information(1)

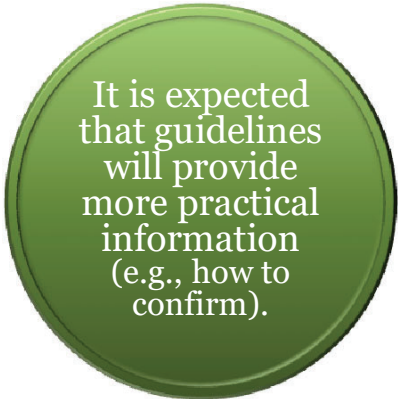
Art. 26-2

- Information of individuals
 - which is not categorized as Personal Information, Anonymously Processed Information, or Pseudonymously Processed Information; and
 - a transferor cannot identify a data subject based on such information; however, a transferee may identify the data subject based on such information together with other information which is available to the transferee.
- This may apply to location information and internet cookies, for example, depending on the situation.

3-2. Personal Related Information(2)

Art. 26-2

- Obligations
 - The updated APPI requires a transferor of Personal Related Information to confirm if a transferee has obtained consent of a data subject to receive Personal Related Information from the transferor
 - Record obligations



It is expected that guidelines will provide more practical information (e.g., how to confirm).

4. Restricted exception for third-party transfers

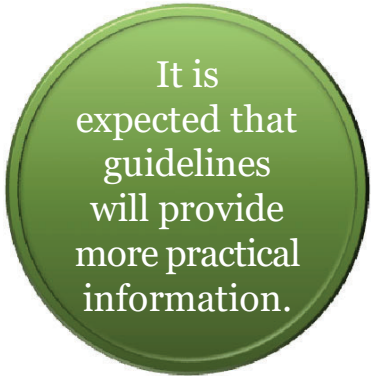
Art. 23 II

- Restricted use of the "opt-out" exception

The revised version of the APPI limits the cases where Data Handlers can use an "opt-out provision" for transfers to third-parties by excluding

- A) Personal Data which is illegally obtained and
- B) Personal Data which is provided based on opt-out provision.

- **More information** is required to be stated where a notification with the PPC is filed to use the opt-out exception



It is expected that guidelines will provide more practical information.

5. Additional obligations for international transfer

Art. 24, 26-2

- If a Data Handler **transfers** Personal Data or Personal Related Information to third parties outside of Japan by way of a **Data Subject's consent** (i.e., not using one of the exceptions), a Data Handler is generally required to provide **certain information** regarding the protection of such transferred Personal Data to the Data Subject.

For example:

- Name of a foreign country
- what sorts/types of data protection measures will be taken by the receiving party
- data protection systems in the country where the receiving party is located, etc.

At present, the scope of required information is somewhat ambiguous and it may be burdensome to provide the information. We expect that guidelines will provide more practical information.

5. Additional obligations for international transfer

Art. 24 III

- If a Data Handler **transfers** Personal Data to third parties outside of Japan by way of a **Data Transfer Agreement**,
 - the Data Handler is required to take necessary actions to make sure that the third parties continuously implement appropriate measures for protection of Personal Data, such as the ones stipulated in the Data Transfer Agreement; and
 - a Data Handler is required to provide **certain information** regarding the necessary actions above to the Data Subject, upon request of the Data Subject.

It is expected that guidelines will provide more practical information.

6. Strengthening of penalties

- The amendment is partially effective since December 2020 regarding penalties.

		Imprison with work	Fine (JPY)
Art. 83 Violation of Order from PPC	Individuals	Up to 1 year	Up to 1 million
	Entity	-	Up to 100 million
Art. 84 Use for Illegal Profit	Individuals	Up to 1 year	Up to 500,000
	Entity	-	Up to 100 million
Art. 85 False Report to PPC	Individuals	-	Up to 500,000
	Entity	-	Up to 500,000

Note: An individual is a natural person.

- If a legal entity committed the crime, the individuals are its directors, agents, or employees.
- A legal entity will also incur punishment, if individuals acted in the course of the entity's business.

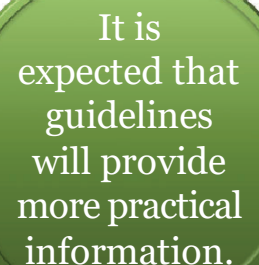
7. More effective extraterritorial applicability Art. 75

- The PPC will be granted more authority towards foreign business operators **which supply goods or services in Japan** and handle Personal Information of individuals in Japan:

- to call for reports (Arts. 75, 40); or
- to issue orders (Arts. 75, 42)

in case of violations of the APPI by the foreign business operator, which can be enforced with a penalty.

The scope is expanded from listed articles to all articles of the APPI.



It is expected that guidelines will provide more practical information.

Check List

1	<input type="checkbox"/> Check current conditions enabling transfer of Personal Data to third party (e.g. opt-out, recording logs).	Strict Opt-out exception in case of data transfer (See 4), Note: effective on October 2021
2	<input type="checkbox"/> Check/establish the reporting system in case of data violations	Introduce reporting obligation to authority (See 2-1)
3	<input type="checkbox"/> Check the work flow to inform affected individuals in case of data violations	Introduce notifying obligation to Data Subjects (See 2-2)
4	<input type="checkbox"/> Consider introducing a periodical check system for international transfers	Restricted conditions on international transfer (See 5)
5	<input type="checkbox"/> Check providing information when obtaining consent from individuals for international transfers, if required	Additional information for Data Subjects when obtaining consent for international transfers (See 5)
6	<input type="checkbox"/> Check the data flow of cookies and other data which may enable a third party to identify a data subject when the third party combines it with their data	Introduce a new concept and obligations for personal-related data (See 3-2)
7	<input type="checkbox"/> Decide whether to use a pseudonymous data scheme	Introduce concept of pseudonymous data (See 3-1)
8	<input type="checkbox"/> Check work flow in case of requests based on individual rights	Expand Data Subject's rights to delete, cease to use/transfer, and to disclose transfer record (See 1)
9	<input type="checkbox"/> Adopt individual rights regarding all personal information, if you use the 6-month retention period exception	Retention-period exception for retained Personal Data no longer applies (See 1 and 3)
10	<input type="checkbox"/> Revise your privacy policy or other internal policy according to 1-9 and obtain consent by April 1, 2022 if appropriate	Fully effective on April 1, 2022

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

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

PPC guidelines and Q & A will likely be issued in

Summer 2021

We will follow up with another webinar

– stay tuned!

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

