Japanese APPI at a glance

NOTE: This material was prepared based on the Amended APPI articles. Thus, until its official enforcement, some provisions might have a gap with the current version of APPI. Article numbers in red are articles that are newly created with the Amended APPI.

Revision History

Version	Contents	Date	Created by
1.0	Released	Aug.12th,2020	Takaya T.
2.0	Major updates: - Examples of PI are added. - Sections of international transfer and children's data are added. - Added cookie consent tool consideration And some other minor updates such as adding comparison with the GDPR for certain terms such as controller and processor.	Aug.20th,2020	Takaya T.

Overview:

Act on the Protection of Personal Information (APPI) is the Japanese privacy law first enacted in 2003 and amended twice. The upcoming amendment will be enacted between April and June 2022. (Note that the penalty provision will come into force in 2020.)

It provides provisions and requirements related to processing of personal data of individuals located in Japan and applies to any enterprise so long as it provides goods or services to individuals in Japan. So, even an entity outside of Japan might fall into the scope of APPI.

Since Japan is the first country that was granted the adequacy decision from the EU after the GDPR implementation in May 25th, 2018, covered entities are, in principle, required to provide "a level of protection essentially equivalent to that guaranteed within the EU".

The English translation of APPI can be found here. (Japanese Law Translation)

The Amendment overview published by the PPC can be found here. (PPC website)

The amended sections of the APPI 2020 version are marked with **Amended**.

Executive Summary of the Amendment of APPI

The major amendments coming from the second APPI amendment are as follows:

- Individuals have a right to suspend the processing or the right to delete their personal data when the processing of retained personal data causes harm to individual rights or legitimate interests.
- Disclosure of retained personal data can be done in electronic format. Previously the format was only defined as "document".
- Disclosure of retained personal data includes record of third-party disclosure.
- Retained personal data includes data that are retained for a short term (i.e. less than six (6) months). Current APPI does not include data deleted within six (6) months, which means current APPI placed additional limitations to individuals for their rights.
- Data breach notification will be mandatory. Notification must be made to the PPC and individuals.
- New definition of "pseudonymously processed information" is introduced to support better utilization of personal data.
- With respect to reidentification at the third-party platform such as DMP, APPI requests a business operator to confirm the lawfulness of the collection to the third parties and to maintain disclosure records.
- The monetary penalties for violation of the PPC's order is reinforced such as fines up to JPY100 million (approx. USD 1.0 mil) for legal entities, which is currently up to JPY 500k (approx. USD 5,000).
- The PPC underlined the fact that entities outside of Japan are also in the scope of order and can be subject to fines by the PPC.

Characteristics of APPI

Based on the OECD Guideline

APPI is based on the OECD Guideline. See the table below to compare the two:

OECD Guideline	APPI
Collection Limitation	Art.16, Art.17,
Data Quality	Art.19
Purpose Specification	Art.15, Art.16
Use Limitation	Art.23, Art.25
Security Safeguards	Art.20, Art.21, Art.22
Openness	Art.18, Art.27
Individual Participation	Art.28, Art.29, Art.30, Art.31, Art.32, Art.33, Art.34
Accountability	Art.35

Unique Definition of PI

APPI classes PI into three categories and applies different requirements to each.

No Definition of Processors

APPI has a concept of "outsourcing" but does not match with the concept of "processor" in the GDPR. For example, at some cases, "outsourcing" companies are not considered as "third-party". (e.g. APPI, Art.23(5))

A business operator is responsible for supervising its outsourcing companies so that they will maintain an equivalent level of safeguards to the outsourced personal data. Contract is used as a tool for this purpose.

Existence of Effort Requirements

APPI has obligation provisions (i.e. organizations MUST follow) and "effort" provisions (i.e. organizations are encouraged to follow). Failure to comply with the provisions categorized as "obligation" is presumed to breach the law and lead to a "recommendation" or an "order". In contrast, failure to comply with the latter group of provisions is NOT presumed to be immediately a breach of the law.

Delegation of Authority

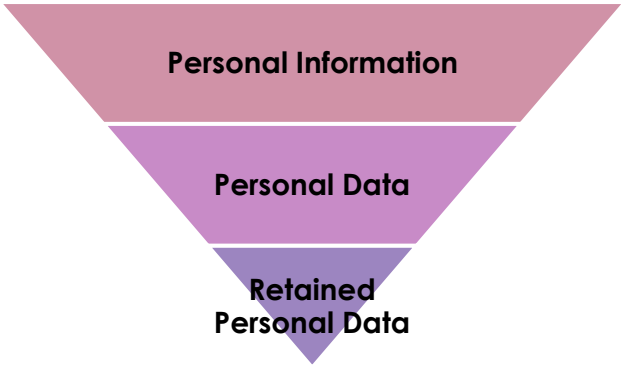
While the **Personal Information Protection Commission** ("**PPC**") supervises the overall enforcement of the law, sector specific enforcements are delegated to a business jurisdictional minister. (APPI Art.44) For example, electrical communication, broadcasting, postal services are overseen by the Ministry of Internal Affairs and Communications and its minister is responsible for publishing guidance guidelines.

Entire list of delegation can be found here. (Japanese only)

Basic Concepts

Definition of PI

The unique categorization of PI is one of the key characteristics of APPI.



APPI categorizes personal information into three groups (plus one special group, which is essentially same as special categories of personal data in the GDPR.)

Obligations are differentiated among them:

Category of Personal Information

- Personal information
- Personal data
- Retained personal data
- Special care-required personal information

Personal information (APPI, Art.2(1))

Personal information (or "PI") means electric or non-electric information relating to an identified or identifiable living individual, such as a name, date of birth, voice, movements, and their combinations. Biometric data and personal identification data are considered as PI. Information about a deceased person and legal person are not considered as PI.

PI that falls into this category shall follow the obligations specified in APPI **Art.15 – APPI Art.18**. (i.e. purpose specifications, purpose limitation, and lawful collection (with consent, privacy notice before collection),

<Examples: (see also Section 2-1, general guideline of APPI)>

- An Individual's first/last name
- Date of birth, contact information (physical address, location, phone number, email address), role in a company, department in a company, where these are combined with an individual's first/last name
- CCTV images that can identify individuals
- Recorded voice that can identify an individual (e.g. when an individual's first/last name is included in the record)
- An email address that can identify an individual (e.g. an email address of john_smith@example.com indicates "john smith" works for company "example".)
- Publicly available information; (e.g. in the official gazette, telephone directory, legal disclosure documents such as securities report, newspapers, websites, SNS.)

Personal data (APPI, Art.2(6))

Personal data means personal information that constitutes a personal information database.

Personal information database (APPI, Art.2(4)) means a collective body of information that comprises of personal information, which can be electric or non-electric and searchable records.

PI that falls into this category shall follow, in addition to APPI Art.15 – APPI Art.18, the obligations specified in **APPI Art.19 – APPI Art.26**. (i.e. data quality, security, data management, disclosure to third-party, and international data transfer).

<Examples: (see also Section 2-4 and 2-6, general guideline of APPI)>

【Personal information database】

- Address book in an email software (when it includes a first/last name and a corresponding email address)
- An electric file that contains users' activity log of web services
- Electrically managed business card information
- A structured filing system of registered professionals

【Personal data】

- PI in a removable device, which is copied from a personal information database
- PI printed on paper, which is outputted from a personal information database

Retained personal data (APPI, Art.2(7)) Amended

Retained personal data is personal data which a business operator has controls over it, such as disclose, correct, delete, or suspension. It excludes personal data whose disclosure might lead to an adverse consequence. (e.g. when a disclosure of personal data might pose threat to someone's life, when a disclosure might lead to social insecurity, etc.) (Current APPI does not include personal data which are supposed to be deleted within six (6) months. Amendment removed this exception and if a business operator has a control over a personal data, it is assumed as retained personal data.)

PI that falls into this category shall, in addition to **APPI Art.15 – APPI Art.26**, follow the obligations specified in **APPI Art.27 – APPI Art.30**. (i.e. right to information, disclosure, correction, cease).

Special care-required personal information (APPI, Art.2(3))

PI that requires special care for handling, such as race, belief, health information, and criminal record are defined as "special care data". This category is essentially equivalent to the definition of the special categories of data in the GDPR. (GDPR, Art.9) Note that PI that allow others to infer of "special care data" (e.g. color of skin) does not consist "special care data".

For handling this category of personal information, special conditions are added, such as explicit consent (APPI Art. 17) and exclusion from the opt-out provision (APPI Art.23(2)).

The table below summarized the requirements of APPI according to its PI category.

	Personal Information	Personal data	Retained personal data
Art.15 Purpose specifications	○	○	○
Art.16 Restriction pursuant to Purpose	○	○	○
Art.17 Lawful collection	○	○	○
Art.18 Transparency in General	○	○	○
Art.19 Data accuracy and Data minimization	N/A	○	○
Art.20 Safeguard	N/A	○	○
Art.21 Employee supervision	N/A	○	○
Art.22 Outsourcing	N/A	○	○
Art.23 Third-party disclosure	N/A	○	○
Art.24 Third-party in foreign countries	N/A	○	○
Art.25 Record keeping	N/A	○	○

Art.26 Receiving data from third-party	N/A	O	O
Art.27 Transparency for retained personal data	N/A	N/A	O
Art.28 Disclosure request	N/A	N/A	O
Art.29 Correction request	N/A	N/A	O
Art.30 Suspension request	N/A	N/A	O
Art.35 Addressing complaint	N/A	N/A	O

A Business Operator

A business operator can be compared with the data controller in the GDPR. The difference with GDPR is that many of the obligations specified in APPI only apply to the private entities. Governmental organizations are excluded from the scope except for the limited area such as individual's right to lodge a complaint. The processing of data by government organizations is covered by sectorial laws. (i.e. Act on the Protection of Personal Information Held by Administrative Organs and Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc.)

A Business operator (APPI, Art.2(5))

Business operator, more precisely **personal information handling private business operator**, is a person processing data in a structured format such as a personal information database for business use. Governmental organizations (central/local) and government agencies are NOT included in this definition. Note that a person may be an individual or legal person.

Handling of PI

There is no definition regarding the handling of personal information, but organizations may apply the definition of the processing definition as provided by the GDPR. (i.e. any activities on personal information, both for electronic records and non-electronic records.)

Trivia:

APPI selected to use "Handling" intentionally to explicitly include processing of non-electronic information. ("processing" was assumed misleading in Japanese that it only covers electronic information.)

Scope of APPI

Exclusion (APPI, Art.76)

As stated above, APPI only applies to the private sector and does not apply to Governmental sector. Also, the following type of organizations are excluded from the scope of APPI.

- Media and press organizations
- Professional writers
- Academic institutions including universities
- Religious bodies
- Political bodies

Extraterritorial Application (APPI, Art.75) **Amended**

APPI applies to any handling of personal information that occurs in Japan, where a business operator supplies goods or services to the Japanese market. Even when a business operator is established outside of Japan, APPI will apply. (With current APPI, entities outside of Japan are not subject to the enforcement actions from the PPC such as request of reporting its PI handling practices or orders to stop handling PI. Amended APPI allows the PPC to do so, which is enforced with a penalty.)

Requirements of APPI

Purpose Specification

Purpose Specification (APPI, Art.15, Art.16)

When handling PI, a business operator must specify the purpose for handling it. Note that a business operator may change the purposes for handling it so long as it is reasonably relevant to original purpose. (APPI, Art.15)

When a business operator would like to expand the purpose of processing and it is irrelevant to original purpose, it must obtain a new consent from each individual. (APPI, Art.16) This consent is not required when the expansion of the purpose is;

- based on laws and regulations
- to protect vital interests of individuals
- to promote public health or childcare
- to support government or government agencies where it is based on legal requirements and revealing the purpose might interfere with their interests

Use Limitation

Providing to Third-party (APPI, Art.23, Art.25)

A business operator can provide its personal data to a third-party only after obtaining a consent from individuals. There are several exceptions where consent is not required:

- based on laws and regulations (e.g. crime investigation) (same as APPI, Art.16)
- to protect vital interests of individuals (same as APPI, Art.16)
- to promote public health or childcare (same as APPI, Art.16)
- to support government or government agencies where it is based on legal requirements and revealing the purpose might interfere with their interests (same as APPI, Art.16)

Examples: (see also 3-4-1, general guideline of APPI)>

【Providing to "third-party"】

- When exchanging personal data between a parent company and a subsidiary company, among fellow subsidiary companies, and among group companies
- When exchanging personal data between a headquarters for a franchise organization and franchisees

The definition of "third-party" in APPI is different from other laws and regulations of the world. APPI says "outsourcing" (e.g. populating data to database, hiring a delivery service to deliver products), "business succession" (e.g. providing personal data to a new company as a result of M&A or business transfer), and "joint handling" (e.g. when a group of companies uses personal data in alignment with the purposes specified at the time of collection, when personal data is used between a parent company and a subsidiary company in alignment with the purposes specified at the time of collection) does not constitutes third-party since it is viewed as one entity from the individuals' perspective. (APPI Art.23 (5))

Once a business operator provides its holding personal data to a third-party, it must keep a record of its disclosure. The record must include the date of disclosure, the name of the third-party, and type of personal data (e.g. first/last name, physical address) and be kept for three years.

Collection Limitation

Lawful Collection (APPI, Art.16, Art.17) Amended

Amended APPI adds a provision that a business operator must handle PI in a lawful and fair way. (APPI, Art.16(2))

When a business operator collects PI, it must not deceive the individuals, nor collect it in an unfair method. (APPI, Art.17(1)) Especially, when a business operator collects special care data (or special categories of personal data), it must obtain explicit consent from the individual. (APPI, Art.17(2)) Even for the collection of special categories of personal data, there are some cases a business operator is not required to obtain consent. These cases are the following, when the collection is:

- based on laws and regulations (same as APPI, Art.16)
- to protect vital interests of individuals (same as APPI, Art.16)
- to promote public health or childcare (same as APPI, Art.16)
- to support government or government agencies where it is based on legal requirements and revealing the purpose might interfere with their interests (same as APPI, Art.16)
- from a public directory published by an individual, a governmental organization (central/local), and other governmental agencies.

- not intrusive such as that characteristics is obvious or necessary in the course of outsourcing, necessary for succession of business, necessary for joint controllership.

Openness

Transparency in General (APPI, Art.18)

When a business operator collects personal information, it must disclose the purpose of collection to individuals. Note that this requirement does NOT apply when the purpose of collection is already disclosed to the public (APPI, Art.18(1)), or one of the following conditions applies:

- based on laws and regulations (same as APPI, Art.16)
- to protect vital interests of individuals (same as APPI, Art.16)
- to promote public health or childcare (same as APPI, Art.16)

Transparency for Retained Personal Data (APPI, Art.27)

When a business operator handles "retained personal data", following information must be provided to individuals:

- the name or appellation of the business operator
- the purpose of handling all retained personal data
- the procedures for responding to a request
- other information specified and required by the government

Data Quality

Data Accuracy and Data Minimization (APPI, Art.19)

A business operator is encouraged to maintain its handling "personal data" accurate and up to date. It must delete "personal data" once the personal data is no longer necessary for its original purpose.

Security

Safeguard (APPI, Art.20, Art.21, Art.22)

A business operator must take necessary and appropriate action to safeguard personal data from personal data breach. (APPI, Art.20) The safeguard measure includes not only providing training and awareness program but also supervision of employees. (APPI, Art.21)

When the business operator outsources some handling of "personal data", it must supervise the outsourcing entities. (APPI, Art.22) Basically, the outsourced entities must apply with the same safeguards / level of protection as that of the outsourcing entity. Note that the outsourcing entities can compare with the data processor of the GDPR, but the concept is vaguer in APPI considering some exceptions specified in APPI. (see also "Providing to Third-party" under the section of "Use Limitation")

Breach Notification (APPI, Art.22(2)(1)) Amended

When a business operator experiences a personal data breach which may violate individuals' rights and interests, the business operator must swiftly notify the PPC and individuals as soon as possible. If a business operator acts as processor (i.e. outsourced organization) and notify to the controller (i.e. outsourcing organization), the business operator is not required to notify the PPC and individuals. (APPI, Art.22(2)(1))

The amended APPI mandates "personal data" breach notification. The timeframe for notification is not specified. The PPC has a dedicated page for breach notification on its website, thus a business operator that experienced a personal data breach would notify the PPC through this page.

Individual Participation

Disclosure Request (APPI, Art.28, Art.32, Art.33, Art.34) Amended

Individuals have a right to request for disclosing "retained personal data" to a business operator. (Art.28(1)) The current APPI specifies the standard disclosing method as disclosure with a "written document", but the amendment allows a business operator to make use of electronical copies or other methods, as specified by the individuals. (Art.28(1))

Amended APPI allows Individuals to obtain a record of "third-party provision" by requesting for the disclosure. (Art.28(5))

Unlike the access requests in the GDPR, when a business operator specifies an application process for the individuals' right request, individuals must follow it to exercise this right. (APPI, Art.32(1))

A business operator may charge to the request. (APPI, Art.33(1))

If a business operator does not respond to the request, individuals are entitled to file to the lawsuit. Individuals must wait for 14 calendar days after the business operator received the request, before filing a request to the court. (APPI, Art.34(2))

Correction Request (APPI, Art.29, Art.32, Art.33, Art.34)

Individuals have a right to request the correction of their "retained personal data" to a business operator. (Art.29(1)) Correction of data includes modifying incorrect contents, deleting incorrect contents, or adding necessary contents.

Those provisions stated at the Disclosure right section (i.e. Requesting process provision (APPI, Art.32(1)), Charging provision (APPI, Art.33(1)), Filing provision (APPI, Art.34(2))) apply to the correction request, as well.

Suspension Request (APPI, Art.30, Art.32, Art.33, Art.34) Amended

Individuals have a right to request for suspending "retained personal data" to a business operator. (APPI, Art.30(1)) Note that the suspension is granted under certain conditions, for instance, breach of purpose limitation (APPI, Art.16(1)), breach of collection limitation (APPI, Art.16(2)) or breach of lawful collection (APPI, Art.17) has occurred. This suspension request can also be justified when the "retained personal data" is no longer needed for its handling purposes, or when data breach occurred, or when handling of the data adversely affects individuals' legitimate interests. (APPI, Art.30(5))

Note that the concept of suspension in APPI includes "deletion" of data. A business operator can select either ceasing to handle it or deleting it when complying with the suspension request.

Accountability

Addressing Complaint (APPI, Art.35)

A business operator is expected to address for individuals' complaints in an appropriate and swift way, by establishing an effective responding system in it. (APPI, Art.35)

This is an "effort" requirement and is not a must-have requirement.

International Transfer of Personal Data

International Transfer of Personal Data

Restriction of Cross-border Transfer (APPI, Art.24(11))

A business operator is NOT allowed to transfer personal data to a third-party outside of Japan unless;

- the business operator obtained consent from an individual
- the third-party is established in the country that has adequate level of protection of personal information
- the business operator and the third-party has concluded an agreement to maintain the same level of the protection as the business operator does.

Japan received an adequacy decision from the EU on July 17th, 2018. It was a so-called "mutual adequacy finding" process and was the first adequacy decision provided by the EC after the GDPR implementation. The PPC published a "supplemental rule" to match the level of PI protection with the EU. Those who imported personal data from the EU and U.K. must follow this rule.

Anonymization and Pseudonymization

Adequacy Decisions

Anonymously processed information (APPI, Art.2(11))

Anonymously processed information means information relating to an individual that can be produced from processing personal information so as neither to be able to identify a specific individual nor to be able to restore the personal information.

To generate anonymized PI, a business operator must follow the specifications prescribed in APPI, Art.36.

Pseudonymously Processed Information (APPI, Art.2(9)) Amended

Pseudonymously processed information means information relating to an individual that can be produced from processing personal information so as not to be able to identify a specific individual unless collated with other information.

The concept of the pseudonymously processed information is newly introduced with the amended APPI. The purpose of introducing pseudonymous PI is to allow businesses to utilize PI in an easier way. Pseudonymous PI may and may not fall into the definition of PI, but when it falls into the definition of PI, many of the requirements of APPI applies, such as purpose specifications, collection limitation, safeguard, and addressing complaints. Still, the flexibility of the pseudonymous PI is expected to benefit businesses.

Re-identification Issue

Re-identification at Third-party (APPI, Art.26(2)) Amended

In the ecosystem of a Data Management Platform (DMP), a business operator might share nonpersonal data with third parties, knowing it might be reidentified after combining with some other information the third parties have. Considering the situation, the amended APPI

mandates a business operator to confirm if the consent is provided by individuals to third parties when such reidentification happen at third parties. At the same time, record of providing such nonpersonal data must be kept by the business operator. (APPI, Art.26(2))

Cookies:

Cookie consent may NOT be requested even under the amended APPI. Some point out article 26 (2) requires a cookie tool, but it only requires a business operator to confirm the existence of "consent" from an individual with the providing third-party where the third-party identifies an individual using the data. Still a business operator needs to use a cookie consent management tool as long as accesses from the EU or U.K. exsit.

Children's Data

No Requirements in APPI

APPI does not have any provisions dedicated for the protection of children's PI. In other words, business operators are NOT required to obtain parental consent from the child's parents or guardians to collect personal information of them.

Trivia:

APPI is based on the OECD guideline 1980 and it is worth pointing out that the OECD guideline published in 1980 did not mentioned to the protection of children. In 2013, the OECD updated its guideline as "OECD Privacy Framework" and it has the sentence below. Hopefully, APPI will incorporate the concept of children's online safety in the near future.

"As children are a particularly vulnerable category of data subjects, Member countries are specifically encouraged to consider privacy literacy initiatives which seek to equip children with the knowledge and skills necessary to stay safe online and use the Internet to their benefit.

(OECD Privacy Framework (2013) pp.31-32)"

Role of the PPC

Overview

The Personal Information Protection Commission ("**PPC**") is an independent data protection authority in Japan. The PPC is responsible for protecting the rights and interests of individuals and promoting appropriate and effective use of PI.

More concretely, the PPC

- create and publish a guidance;
- supervises over the handling of PI;
- establishes rules;
- provides mediation for lodged complaints;
- cooperates with foreign DPAs; and
- other tasks specified by the law.

You can find guidance published by the PPC here: (Japanese)

Enforcement Power and Penalty **Amended**

The PPC has an enforcement power. Its enforcement power includes;

- requiring a business operator to report or submit necessary information or material (APPI, Art.40(1));
- performing on-site inspections (APPI, Art.40(1));
- providing guidance or advice (APPI, Art.41);
- providing recommendation (APPI, Art.42(1)); and
- placing an order (APPI, Art.42(2)(3)).

The PPC has not been active about taking enforcement actions. The first order ever made by the PPC was on July 29th, 2020, whereas the PPC was established in 2016. The order was issued to the operators of two websites that have listed the names of individuals who have declared personal bankruptcy. These two websites breached the provisions of APPI, Art.18 (disclosure of purposes) and APPI, Art.23(1) (third-party disclosure).

When a business operator or an individual violates APPI, both the business and the individual that violated APPI are punished and fined. (APPI, Art.87)

The relationship among enforcement actions and penalties is summarized in the table below:

Enforcement	Violation	Fine	Dual Liability
Reporting / Submission of information or material (APPI, Art.40(1))	Fail to submit a report or material, or falsely submit a report	Up to JPY 500k (approx. USD 5,000-) (APPI, Art.85)	Yes
On-site inspection (APPI, Art.40(1))	Failed to answer a question or did falsely answer a question, or refused, obstructed or evaded an inspection	Up to JPY 500k (approx. USD 5,000-) (APPI, Art.85)	Yes
Guidance / Advice (APPI, Art.41)	N/A	N/A	N/A
Recommendation (APPI, Art.42(1))	Art. 16 - 18, Art. 20 – 22(2), Art. 23 (excl. (4)), Art. 24 – 25, Art. 26 (excl. (2)), Art. 27, Art. 28 (excl. (1)), Art. 29(2)(3), Art. 30 (2)(4), (5), Art 33 (2), Art. 36 (excl. (6))	N/A	N/A
Order (APPI, Art.42(2)(3))	Art. 16 - 17, Art. 20 - 22, Art. 23 (1), Art. 24, Art. 36 (1) (2) (5), Art.38	[Individuals] Up to JPY 1 mil (approx. USD 10k-) or up to one year of imprisonment (APPI, Art.83) [Businesses] Up to JPY 100mil (approx. USD 1mil) or up to one year of imprisonment (APPI, Art.87)	Yes
Others	Art.26(2), Art.55	Up to JPY 100k (approx. USD 1,000-)	

PrivacyMark® (Certification)

What is the PrivacyMark®?

PrivacyMark® logo

PrivacyMark®, or "**P-Mark**", is a certification system in Japan. Assessment of the certification is performed based on JIS Q 15001, which is a standard for personal information protection management system. You may compare JIS Q 15001 with BS 10012 but JIS Q 15001 is specifically designed to comply with APPI.

PrivacyMark® is operated and managed by **JIPDEC**, or Japan Institute for Promotion of Digital Economy and Community, since April.1st, 1998. JIPDEC has a close relationship with the central government and plays an important role in Japanese privacy world. As of August 13th, 2020, as many as 16,419 entities are certified. The P-Mark is prevailing in Japan and many business operators request their outsourcing parties to be certified, as a proof of appropriate safeguard.

Requirements in JIS Q 15001

As stated above, PrivacyMark® is certified based on JIS Q 15001. In general, JIS Q 15001 sets higher and detailed standards or requirements for PI protection compared with APPI.

Here are two examples that the JIS Q 15001 sets a higher requirements than those of APPI.

Conducting PIA (JIS Q 15001:2017, 3.3.3)

A business operator must conduct PIA to identify and analyze the risk pertaining to its PI handling practices. The business operator is expected to establish and maintain necessary and appropriate safeguards based on the results of the PIA, which are reviewed, at least, once a year.

Appointment of DPO (JIS Q 15001:2017, 3.3.4)

JIS Q 15001 requires the top management of an organization to appoint a DPO and an internal auditor. The DPO is responsible for reporting to the top management about the status of PI protection in the organization. The internal auditor shall conduct the audit and report to the top management.

APPI and the GDPR

Since the GDPR has established a global standard for the data protection regime, you may find it useful to compare APPI with the GDPR. The table below shows a general comparison among the OECD Guideline, APPI, and the GDPR.

OECD Guideline	APPI	GDPR
Collection Limitation	Art.16, Art.17,	Art.5(1)(a), (b)
Data Quality	Art.19	Art.5(1)(b), (d), (e)
Purpose Specification	Art.15, Art.16	Art.5(1)(b)
Use Limitation	Art.23, Art.25	Art.5(1)(b)
Security Safeguards	Art.20, Art.21, Art.22	Art.5(1)(f)
Openness	Art.18, Art.27	Art.5(1)(a), Art.12, Art.13, Art.14
Individual Participation	Art.28, Art.29, Art.30, Art.31, Art.32, Art.33, Art.34	Art.5(1)(a), Art.12, Art.15, Art.16, Art.17, Art.18
Accountability	Art.35	Art.5(2)

Useful Links

The Personal Information Protection Committee:

https://www.ppc.go.jp/

APPI (Japanese - English):

http://www.japaneselawtranslation.go.jp/law/detail/?id=2781&vm=04&re=01

Promulgated Amendment of APPI (Comparative table):

https://www.ppc.go.jp/files/pdf/20200612_comparative_table_amended_APPI.pdf

Promulgated Amendment of APPI (Overview):

https://www.ppc.go.jp/files/pdf/overview_amended_act.pdf

PrivacyMark®:

https://privacymark.org/

About the Author

Takaya Terakawa (CEO, Technica Zen) (CIPP/E, CIPM)

Takaya Terakawa is a security, data privacy and data governance consultant, lecturer, and trainer in Japan. Takaya runs his own enterprise, Technica Zen. Takaya is one of the most trusted data privacy professionals in Japan who understands both security and privacy perspectives, with hands-on experiences of governance administration in organizations. His recent work involves consulting on the ISMS certification, the PIMS certification, GDPR compliance, acting as anexternal DPO, and is an advisor of APAC privacy trends.

Takaya also has written a textbook on data privacy. His second book on privacy management program is expected to be published at the end of 2020. Takaya is also an advocate of children's online safety and Head of Country, Japan, for The Cybersafety Group.

IAPP knowledgeNet Tokyo co-chair: 2018 - 2020

Expert Advisor of JETRO: 2018 – Present

LinkedIn: https://www.linkedin.com/in/takaya-terakawa-567b1348/

Website: https://technica-zen.com/ (Japanese)