



The Legal 500 & The In-House Lawyer  
Comparative Legal Guide  
Japan: Data Protection & Cyber Security

This country-specific Q&A provides an overview to data protection and cyber security laws and regulations that may occur in [Japan](#).

This Q&A is part of the global guide to Data Protection & Cyber Security. For a full list of jurisdictional Q&As visit <http://www.inhouselawyer.co.uk/practice-areas/data-protection-cyber-security/>



**Country Author: Atsumi & Sakai**

The Legal 500



**Fumiaki Matsuoka, Partner,  
Lawyer, (admitted in Japan)**

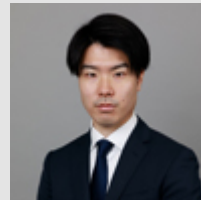
[fumiaki.matsuoka@aplaw.jp](mailto:fumiaki.matsuoka@aplaw.jp)

The Legal 500



**Maki Katayanagi, Associate,  
Lawyer (admitted in Japan)**

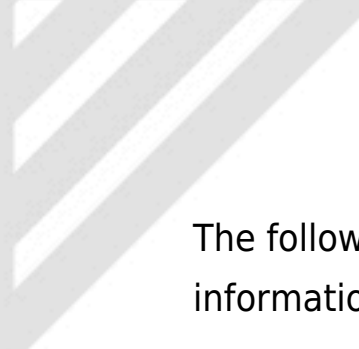
[maki.katayanagi@aplaw.jp](mailto:maki.katayanagi@aplaw.jp)



**Satoshi Fukuhara,  
Associate, Lawyer  
(admitted in Japan)**

[satoshi.fukuhara@aplaw.jp](mailto:satoshi.fukuhara@aplaw.jp)

- 1. Please provide an overview of the legal framework governing privacy in your jurisdiction (e.g., a summary of the key laws, who is covered by them, what sectors, activities or data do they regulate, and who enforces the laws enforced)?**



The followings are the relevant rules concerning personal information protection in Japan:

1. Act on the Protection of Personal Information (“APPI”);
2. Act on the Protection of Personal Information Held by Administrative Organs;
3. Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc.;
4. Ordinance on the Personal Information Protection of Rules for Local Governments; and
5. Various guidelines.

An overview of each law is as follows:

The law (1) above (i.e. APPI) stipulates the basic policies for the protection of personal information in the public and private sectors, and general rules such as obligations and penalties for the private sector.

The law (2) above stipulates personal information protection policies for the national government agencies, law (3) above stipulates comparable policies for the independent administrative corporations, and the ordinance (4) above stipulates general rules of local governments.

The guidelines in (5) above are administrative guidelines on the interpretation of APPI.

The entity in charge of enforcing laws (1) to (3) above is the national government, while local governments enforce ordinance (4) above

and the guidelines in (5) are open to interpretations and they are not subject to enforcement.

**2. Are there any registration or licensing requirements for entities covered by these laws and, if so, what are the requirements? Are there any exemptions?**


As a system for evaluating and certifying business operators who aim to comply with applicable standards for the establishment of personal information protection systems, there are the (i) JIS Q 15001, Privacy Mark system, and (ii) APEC (Asia-Pacific Economic Cooperation)/ CBPR (Cross Border Privacy Rules) system.

APPI only stipulates rules to be observed, and does not set forth specific procedures for the protection of information. Therefore, as a policy for the establishment of such system, there are many personal information protection management systems introduced so far. The standard evaluation/certification system in Japan is JIS Q 15001, Privacy Mark System. On the other hand, APEC/ CBPR system is designed for cross-border data processing.

**1. JIS Q 15001 Privacy Mark System**

JIS Q 15001 is a standard personal information management system in the field of personal information protection in Japan.

If a business operator establishes a system for proper personal information protection in accordance with JIS Q 15001, it can



apply for and obtain a Privacy Mark after going through an assessment by JIPDEC (Japan Information Processing Development Center).

## 2. APEC/ CBPR System

The CBPR system is a system that certifies compliance with the APEC Privacy Framework for initiatives by companies in relation to the cross-border protection of personal information, etc., in which Japan is also participating.

Business operators who wish to participate in CBPR are required to establish and enforce a personal information protection policy that meets the APEC Privacy Framework, and they are also required to be evaluated for compliance with requirements of a relevant accountability agent in the participating country.

As a general rule in Japan, a business operator handling personal information must obtain the consent of the data subject in advance to enable the provision of personal data to a third party in a foreign country. However by obtaining the CBPR certification, the business operator will be able to bypass this general rule.

## 3. **How do these laws define personally identifiable information (PII) versus sensitive PII? What other key definitions are set forth in the laws in your jurisdiction?**

1. The definition of personal information is stipulated in Article 2, Paragraph 1 of APPI.

## (Definitions)

Article 2 The term "personal information" as used in this Act shall mean information about a living individual applicable to any of the following items:

(i) information containing a name, date of birth, or other descriptions, etc. (meaning any and all matters (excluding an individual identification code) stated, recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record (meaning a record kept in an electromagnetic form (meaning an electronic, magnetic or other forms that cannot be recognized through the human senses; the same shall apply in the succeeding paragraph, item (ii)); the same shall apply in Article 18, paragraph (2)); hereinafter the same) whereby a specific individual can be identified (including those which can be readily collated with other information and thereby identify a specific individual); or

(ii) information containing an individual identification code.

2. The definition of special care-required personal information is stipulated in Article 2, Paragraph 3 of APPI, and Article 2 of the Cabinet Order.

## Article 2, Paragraph 3 of APPI

3. "Special care-required personal information" in this Act means personal information comprising a data subject's race, creed, social status, medical history, criminal record, fact of having suffered damages by a crime, or other descriptions, etc. designated by a cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the data subject.

## Article 2 of the Cabinet Order

(Special care-required personal information)

Article 2 The descriptions, etc., referred to by the Cabinet Order stipulated in Article 2, Paragraph 3 of APPI shall be descriptions, etc., that contain any of the following matters (excluding those that would qualify as a person's medical history or criminal background):

(i) Physical disabilities, mental disabilities, mental disorders (including developmental disorders), or other mental or physical functional disorders as defined by rules of the Personal Information Protection Commission;

(ii) Results of medical examinations and other tests (referred to as "medical examinations, etc." in this same item) of data subjects for the prevention and early detection of diseases conducted by doctors and other persons engaged in medical-related duties (referred to as "doctors, etc." in the succeeding item);

(iii) Guidance, medical treatment or dispensing medicines for the improvement of mental and physical conditions of the data subject by doctors, etc. based on the results of medical examinations, etc. , illness, injury or other mental or physical changes;

(iv) Procedures related to arrest, search, seizure, detention,

prosecution and other criminal cases involving the data subject as the suspect or accused; or

(v) Procedures related to investigations, measures for observation and protection of juveniles, hearings and decisions, protective measures and other juvenile protection cases involving the data subject as the juvenile or suspected person as stipulated in Article 3, Paragraph 1 of the Juvenile Act (Act No. 168 of 1947).

#### 4. Other key Definition: Personal data

"Personal data" means personal information which constitutes a personal information database. Under Japanese law, the terms "personal data" and "personal information" are defined separately. The law imposes special obligations on business operators that handle personal data. This is because personal data requires a greater level of protection than personal information.

4. **Are there any restrictions on, or principles related to, the general processing of PII - for example, must a covered entity establish a legal basis for processing PII in your jurisdiction or must PII only be kept for a certain period? Please outline any such restrictions or "fair information practice principles" in detail?**

Although there is no legal basis for processing personal data as in Article 6 of GDPR, to process personal information in Japan it is

necessary to comply with the rules of Specifying a Utilization Purpose (Article 15, APPI), Restriction due to a Utilization Purpose (Article 16, APPI), Proper Acquisition (Article 17, APPI), and Notification, etc. of a Utilization Purpose when Acquiring (Article 18, APPI).

In addition, a business operator handling personal data shall strive to keep personal data accurate and up to date within the scope necessary to achieve a relevant utilization purpose, and to delete the personal data without delay when its utilization has become unnecessary (Article 19, APPI).

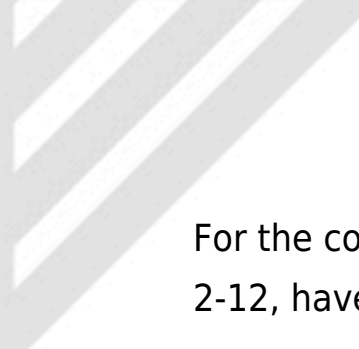
**5. Are there any circumstances where consent is required or typically used in connection with the general processing of PII and, if so, are there are rules relating to the form, content and administration of such consent?**

1. The circumstances where consent is required or typically used in connection with the general processing of PII

The following circumstances require consent for the processing of PII:

1. When using personal information for purposes which the data subject has not been informed of and not disclosed on a website (Article 16 and Article 18, APPI);
  2. When acquiring special care-required personal information (Article 17, Paragraph 2, APPI); and
  3. When providing personal data to a third party (Article 23, Paragraph 1, and Article 24, APPI).
2. Rules concerning the form, content and administration of such consent





For the consent of the data subject, the Guidelines (General Rules), 2-12, have the following provisions:

“Consent of the data subject” means an indication of the intention of the person concerned that he/she consents to having the personal information about the person processed through the processing method indicated by the business operator (on the premise of confirmation of said data subject).

In addition, “Acquiring the consent of the data subject” means the personal information business operator recognizing that the data subject's consent is expressed , and it must be made in a reasonable and proper manner deemed necessary to make a judgment on the data subject’s consent depending on the nature of the business and the status of personal information processing.

Furthermore, if a person does not have the ability to properly assess the consequence of providing consent to the processing of personal information because of his or her status as a minor, an adult ward, a person under curatorship, or a person under assistance, it is necessary to obtain consent from a person who has parental authority over or is a legal representative, etc. of the data subject

In addition, examples of obtaining consent of a data subject are as follows.

Example 1. Data subject indicating its intention through verbal

consent.

Example 2. Receipt of written consent (including electromagnetic records) from the data subject.

Example 3. Receipt of an email containing consent of the data subject.

Example 4. The data subject checking in the confirmation column of consent.

Example 5. The data subject clicking on the button on a homepage to indicate its consent.

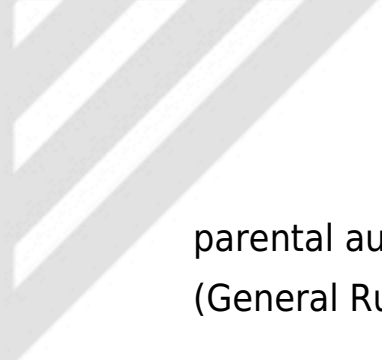
Example 6. The data subject providing inputs such as by voice inputs, touching a touch panel, button or switch, etc. to show its consent.

**6. What special requirements, if any, are required for processing sensitive PII? Are there any categories of PII that are prohibited from collection?**

1. Special requirements for special care-required personal information
  - As a general rule, it is necessary to procure prior consent to collect special care-required personal information from the data subject
2. Special care-required personal information that is prohibited from being collected  
Not applicable.

**7. How do the laws in your jurisdiction address children's PII?**

If a person who is a minor does not have the ability to properly assess the consequence of consenting to the processing of personal information, it is necessary to obtain consent from a person who has



parental authority or is the legal representative, etc. (Guidelines (General Rules), 2-12).

If the data subject is a minor, a legal representative may make a request for disclosure, correction, or suspension of use, etc. (Article 32, Paragraph 3, and Article 11, Item 1 of the Cabinet Order.

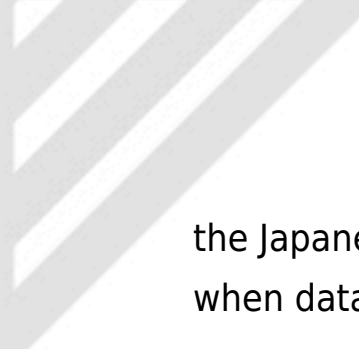
8. **Are owners or processors of PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these requirements.**

When an owners or processors of PII transfers personal information to a third party or receives it from a third party, it must create and save a record of the transfer (Article 25, 26, APPI). On the other hand, there are no general recording obligations like the obligations under Article 30 of GDPR.

9. **Are consultations with regulators recommended or required in your jurisdiction and in what circumstances?**

No.

However, companies often voluntarily consult with Personal Information Protection Commission when they are not sure of how



the Japanese personal data protection act shall be interpreted or when data breach occurs.

- 10. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in what circumstances? How are these risk assessments typically carried out?**

APPI has no provisions which prescribe how risk assessments related to personal information ought to be carried out, nor are such assessments covered under other laws, so there is no legal obligation to conduct risk assessments. In practice, some companies elect to voluntarily carry out risk assessments as part of efforts to avoid data breach.

- 11. Do the laws in your jurisdiction require appointment of a data protection officer, or other person to be in charge of privacy or data protection at the organization? What are the data protection officer's legal responsibilities?**

While there is no legal obligation to appoint a person to be in charge of data privacy, in practice, it is common for business operators to appoint a "Personal Information Protection Manager" within their organizations who has a certain level of authorities and responsibilities for protecting personal information.

12. **Do the laws in your jurisdiction require providing notice to individuals of the business' processing activities? If so, please describe these notice requirements (e.g. posting an online privacy notice).**

Article 18 of the APPI imposes an obligation upon companies requiring that they notify the data subject of the purpose of use of their personal data when they collect the personal information. In principle, companies can use their websites to notify the data subjects of said purpose and in practice they often list the purpose on their privacy policies.

In addition, when acquiring personal information from a data subject via documents such as an application form or a questionnaire, companies need to clearly explain to the data subject the purpose of acquiring their personal information.

13. **Do the laws in your jurisdiction apply directly to service providers that process PII, or do they typically only apply through flow-down contractual requirements from the owners?**

The laws are directly applicable to service providers. For example, service providers have a legal obligation to provide secure management of personal information (APPI, Article 20). Also, service providers must execute a service agreement and pursuant to such service agreement, are contractually obligated to protect personally identifying information (APPI, Article 22).

14. **Do the laws in your jurisdiction require minimum contract terms with service providers or are there any other restrictions relating to the appointment of service providers (e.g. due diligence or privacy and security assessments)?**

APPI itself does not expressly require a minimum contract terms as does Article 28 GDPR. However, Japanese companies usually execute certain contractual documents under APPI and guidelines. The details are as follows.

In cases where a company entrusts a service provider with the handling of personal information, in whole or in part, the company must supervise, as is necessary and appropriate, the service provider entrusted with the handling of the personal information, in order to ensure the secure management of the personal data which has been entrusted thereto (APPI, Article 22). Specifically, the service provider must be appropriately selected, a service agreement must be concluded, and the company must be aware of the status of the personal data handling by the service provider.

Under the Guidelines, it is desirable for the company to conduct regularly scheduled audits of the service provider. Also, in cases where entrusted personal data is leaked as a result of the company's entrustment of personal data to an outside vendor without being aware of the status of its data handling, the company will be deemed not to have carried out the necessary and appropriate supervision of said external vendor(Guidelines for APPI

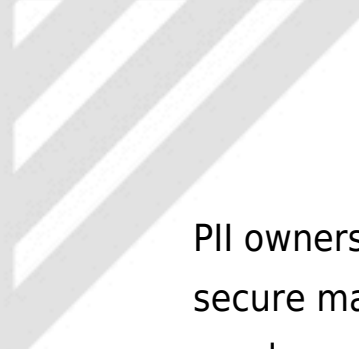
(General Rules Edition) 3-3-4).

15. **Is the transfer of PII outside the jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (for example, does cross-border transfer of PII require notification to or authorization from a regulator?)**

When a company transfers personal data to a third party located outside of Japan, one of the following four conditions must be satisfied (APPI, Article 24).

1. The third party which is in a country listed under the Enforcement Rules for APPI (“Enforcement Rules) as a country with a personal information protection system at a level on par with the Japanese system. With regard to this condition, Japan regards the EU as a region with a personal information protection system on par with its own system.
2. The third party has a system in place which, as a system necessary for the continuous implementation of measures on par with the measures that should be implemented by a company, is a system sufficient under the standards provided in the Enforcement Rules. For example, it is possible to satisfy this condition when, in cases where data is shared with a foreign company, a data protection agreement is concluded. On the other hand, when personal data is shared among multinational companies in the world, if they have appropriate privacy policies, this also would satisfy the condition for data sharing with a third party in a foreign country.
3. When transfer of data to a foreign country is required under law or regulation, or necessary for protection of human life, health, or property, and obtaining the consent of the data subject is difficult.
4. When the data subject provides consent.

16. **What security obligations are imposed on PII owners and on service providers, if any, in your jurisdiction?**



PII owners and service providers are obligated to implement general secure management measures, and are obligated to supervise the employees of their own company (APPI, Articles 20 and 21).

Also, PII owners are obligated to supervise service providers (APPI, Article 22).

17. **Does your jurisdiction impose requirements of data protection by design or default?**

The concept of “by design or default” is not employed under Japanese law.

18. **Do the laws in your jurisdiction address security breaches and, if so, how does the law define “security breach”?**

“Security breach” is not defined under APPI. However, as described in detail in our response to Question 19 (below), the Guidelines’ provisions do address security breach, and these are followed by many companies.

19. **Under what circumstances must a business report security breaches to regulators, to individuals, or to other persons or entities? If breach notification is not required by law, is it**



**recommended by the regulator and what is the typical custom or practice in your jurisdiction?**

The term “Security breach” is not defined under Japanese law, and said concept is also not regulated under the law. However, the guideline on security breach recommends that when there is a leak, loss, or damage (or risk thereof) of personal data held by a PII owner, the PII owner should contact the individuals who may be affected by the leak, loss, or damage, etc. and should report the incident to the Personal Information Protection Committee and to the potentially-affected individuals.

20. **Do the laws in your jurisdiction provide individual rights, such as the right to access and the right to deletion? If so, please provide a general description on what are the rights, how are they communicated, what exceptions exist and any other relevant details.**

Under APPI, an individual has the right to take the following actions: demand disclosure (APPI, Article 28); demand a correction of details of personal data held that are not factually accurate (APPI, Article 29); demand a suspension of use when the relevant data is handled or was obtained in violation of the APPI (APPI, Article 30); and in the event that the individual’s requests are not complied with, the individual may demand an explanation of the reason for such noncompliance (APPI, Article 31).

However, there are certain grounds for refusal of the individual’s

disclosure requests (such as when such information disclosure would pose a risk of injury or damage to the life, body, property, or other rights and interests of the data subject or a third party).

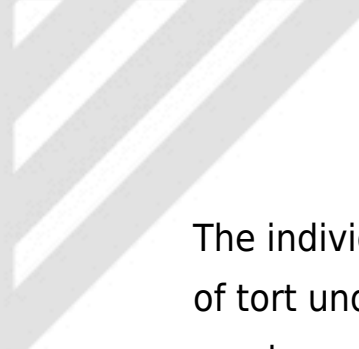
On the other hand, the APPI lacks following provisions which exist in the GDPR: the right to erasure (GDPR, Article 17); the right to data portability (GDPR, Article 20); and the right to object profiling (GDPR, Article 22).

21. **Are individual rights exercisable through the judicial system or enforced by a regulator or both? When exercisable through the judicial system, does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances? Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury of feelings sufficient?**

1. The exercise of rights

With regard to the exercise of rights by individuals, under Article 34 of the APPI, it is possible to file a lawsuit. Specifically, after the individual has requested a disclosure, etc. outside of court, and the two weeks ( the time period viewed as necessary for the business operator to respond to a disclosure request, etc.) have passed, or if the business operator declines the individual's request, the APPI allows the individual to file a lawsuit.

2. Monetary damages or compensation



The individual may pursue a claim for damages based on the theory of tort under the Civil Code. However, in recent years, in most of the court precedents, even when the individual is able to pursue a claim, the amounts which the courts granted for the damages claims have been rather small when there is only an injury to one's emotion found.

**22. How are the laws governing privacy and data protection enforced? What is the range of fines and penalties for violation of these laws? Can PII owners appeal to the courts against orders of the regulators?**

With regard to the enforcement of the APPI, the supervision of PII owners is basically centralized to the Personal Information Protection Committee ("the Committee"). The Committee has the authority to demand reports to be produced by business operators and conduct on-site inspections (APPI, Article 40), and may provide guidance or advice (APPI, Article 41), make recommendations and issue orders (APPI, Article 42), and PII owners who violate certain provisions may be subject to criminal penalties (APPI, Articles 84, 85(i), and 87).

If, with regard to the reporting obligation and on-site inspections by the Committee, the PII owner subject to the reporting requirement or on-site inspection has any complaints, such PII owner may demand an administrative review pursuant to the Administrative Complaint Review Act, or may request the revocation of the

administrative action under the Administrative Case Litigation Act.

The PII owner subject to the administrative guidance, advice or recommendations may request that such administrative guidance, advice or recommendations to be suspended under Administrative Procedure Act, Article 36-2. However, these will not be subject to, a request for review under the Administrative Complaint Review Act or the Administrative Case Litigation Act.

Additionally, if a PII owner violates an order (APPI, Article 42.2), pursuant to the rules of criminal procedure, such PII owner may file complaints against any imposition of fines or imprisonment.

23. **Does the law include any derogations, exclusions or limitations other than those already described? Please describe the relevant provisions.**

Under the APPI, certain “specified PII owners”, when handling personal information for the legally- defined purposes of their various individual businesses, are not subject to some of the obligations provided in the APPI (APPI, Article 76).

Examples of such “specified PII owners” who are not subject to the APPI would be the news media, writers, organizations conducting academic research, religious organizations, and political organizations.

24. **Please describe any restrictions on monitoring or profiling in your jurisdiction including the use of tracking technologies such as cookies - how are these terms defined and what restrictions are imposed, if any?**

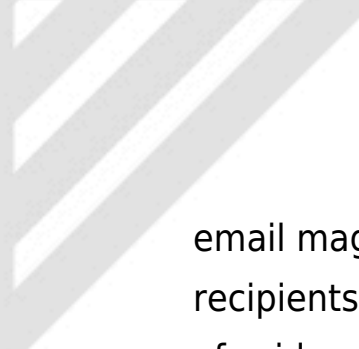
Under the APPI, online identifiers (IP address, cookies, etc.) and location information alone, in and of itself, does not constitute “personal information” (APPI, Article 2.1(i)).

However, in exceptional cases, when such information can be easily matched with other information, and when, through such matching, it becomes possible to identify specific individuals, such information falls under “personal information”, and becomes subject to regulation under the APPI.

25. **Please describe any laws addressing email communication or direct marketing?**

Email communications and direct marketing are regulated under the APPI and the Act on Regulation of Transmission of Specified Electronic Mail (hereinafter “ARTSEM”).

The information about readers of email magazines (name, date of birth, address, etc.) handled by the email magazine operators falls under the definition of “personal information” under Article 2 of the APPI, so the APPI is applicable. When the APPI applies, senders of



email magazine will be required to either directly notify the recipients of the email magazine or publicly post the purpose of use of said personal information (APPI, Article 18). The email magazine recipients may request that the senders suspend the use or delete the personal information (APPI, Article 30).

Also, ARTSEM requires that the senders, when sending out email magazines, “obtain an opt-in” from recipients (ARTSEM, Article 3.1); and have an “opt-out mechanism” (ARTSEM, Article 3.3). “Obtain an opt-in” means that the senders obtain the recipient’s consent before sending the respective emails. “Opt-out mechanism” means a mechanism which enables recipients to notify and request senders to stop sending emails even after the sender has obtained the opt-in from the recipient if, at a later time, the recipient no longer desires to receive such emails. Penalties are provided for violations of the foregoing requirements (ARTSEM, Article 33 et seq.)