Would you consider your national data protection laws to be ahead or behind of the international curve?

Japan

The key legislation governing personal information and data in Japan is the Act on the Protection of Personal Information (57/2003).

An amendment bill was passed in September 2015 and, as a result, the act has been updated to reflect modern society and international data protection laws. For example, the Personal Information Protection Commission (PPC) was established as Japan’s privacy commissioner on January 1 2016.

However, because there are many ambiguous provisions and pending issues in the amended act, Japan’s national data protection laws remain behind the international curve.

Are any changes to existing data protection legislation proposed or expected in the near future?

Japan

The amended Act on the Protection of Personal Information will come into effect as of the date specified by cabinet order (within two years of the date on which the bill was issued).

Details of the amended act will be provided by cabinet order or in the PPC rules that will hopefully be issued in 2016. Parties are therefore advised to monitor further developments.

What legislation governs the collection, storage and use of personal data?

Japan

The key legislation governing the collection, storage and use of personal information in Japan is the Act on the Protection of Personal Information. The act provides the general rules concerning the protection of personal information in the private sector and regulates the handling of personal information.

Who falls within the scope of the legislation?

Japan

The Act on the Protection of Personal Information applies to ‘business operators handling personal information’ – defined in the act as any person using a personal information database for business (for further details please see the following question) that has held the personal information of more than 5,000 unique individuals at any time in the past six months.
The act does not apply to:

- state organs;
- local governments;
- incorporated administrative and similar agencies;
- local independent administrative institutions; and
- entities specified by cabinet order as having little likelihood of harming the rights and interests of individuals considering the volume of personal information that they handle and the manner in which they utilise it (ie, small business operators).

Article 2 of the Cabinet Order on the Act on the Protection of Personal Information defines a ‘small business operator’ as an entity that uses for business a personal information database containing a combined maximum of 5,000 unique individuals at any time in the past six months. However, the amended act will remove this exception.

A foreign entity may constitute a ‘business operator handling personal information’ under the Act on the Protection of Personal Information if it has business entities or a branch in Japan.

What kind of data falls within the scope of the legislation?

The Act on the Protection of Personal Information applies to three categories of information and data, each of which is governed by different rules:

- ‘Personal information’ – information about a living individual that can be used to identify the individual through his or her name, date of birth or other description contained in the information (including information that allows easy reference to other information that would thereby enable identification of the individual).
- ‘Personal data’ – personal information contained within a personal information database. A ‘personal information database’ is a collection of information, including:
  - a collection of information systematically arranged in such a way that enables specific personal information to be retrieved from it by a computer; and
  - any other collection of information designated by the cabinet order as being systematically arranged in such a way that enables specific personal information to be easily retrieved from it (ie, if the personal information is organised according to certain rules or if a table of contents, index or other arrangement aids retrieval of the personal information).
- ‘Retained personal data’ – personal data that a business operator governed by the act has the authority to:
  - disclose;
  - correct;
  - add to or subtract from;
  - discontinue the utilisation of;
  - erase; or
  - discontinue the provision of to a third party.

The cabinet order specifies certain data that is excluded from the definition of ‘retained personal data’ – namely because knowledge of it would be harmful to the public or another interest or because it will be erased within six months.

New types of information – including personal identification codes – will be added to the definition of ‘personal information’ in the amended Act on the Protection of Personal Information. A ‘personal identification code’ is a code that can be used to identify an individual. Examples of personal identification codes – to be specified in a cabinet order – include biometric identifiers such as fingerprint and face recognition data and passport and licence numbers. As it is unclear at present whether this information counts as ‘personal information’ and ‘personal data’, the amendment has clarified that it does.

In addition, the amended Act on the Protection of Personal Information will govern the processing method and handling of ‘anonymised processed information’ – information about an individual obtained by processing personal information in such a way that the individual is not identified. It will also restrict the restoration of such information, pursuant to the act and the Personal Information Protection Commission (PPC) rules.

Are data owners required to register with the relevant authority before processing data?
Is information regarding registered data owners publicly available?

Japan

Not applicable.

Is there a requirement to appoint a data protection officer?

Japan

There is no legal requirement to appoint a data protection officer under the Act on the Protection of Personal Information and applicable guidelines. However, business operators governed by the act must take security control measures concerning personal data and the appointment of a data protection officer is provided as an example of ‘organisational measures’, which is one of the security control measures provided for by some guidelines.

Enforcement

Which body is responsible for enforcing data protection legislation and what are its powers?

Japan

The Act on the Protection of Personal Information is enforced in each industry by the relevant regulatory ministry. The majority of Japanese businesses are regulated by:

- the Ministry of Economy, Trade and Industry;
- the Ministry of Health, Labour and Welfare;
- the Financial Services Agency;
- the Ministry of Internal Affairs and Communications; or
- the Ministry of Land, Infrastructure and Transport.

Each ministry may request reports on the handling of personal information and issue recommendations or orders to business operators that violate the Act on the Protection of Personal Information. Non-compliance with a request or violation of an order can result in fines, imprisonment or both.

Once the amended Act on the Protection of Personal Information takes effect, the PPC will be responsible for its enforcement in the private sector. The PPC will be able to request reports and issue recommendations and orders, as well as conduct on-the-spot inspections.

Collection and storage of data

In what circumstances can personal data be collected, stored and processed?

Japan

Processing

A business operator governed by the Act on the Protection of Personal Information must specify the purpose of use for personal information it handles (to the extent possible) and comply with the following rules:

- it must not change the purpose of use beyond a scope which has a reasonably substantial relation to the original purpose of use; and
- it must not use the personal information beyond the scope necessary to achieve the purpose of use, without
obtaining the individual’s prior consent.

The word ‘substantial’ will be removed from the first requirement in the amended Act on the Protection of Personal Information, which will instead read “a scope which has a reasonable relation to the Purpose of Use before the change”.

**Collection**

The following restrictions apply to the collection of personal information by business operators governed by the Act on the Protection of Personal Information:

- **proper acquisition** – a business operator must not acquire personal information by deception or other wrongful means;
- **notice of purpose of use at time of acquisition** – once a business operator has acquired personal information, it must notify the individual of or publicly announce the purpose of use unless it has already been publicly announced or one of the following applies:
  - such notification or public announcement would likely cause harm to the life, body, property, rights or interests of an individual or third party;
  - such notification would likely harm the business operator’s rights or legitimate interests;
  - cooperation with a state agency, local government or third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and the notification or public announcement of the purpose of use would likely impede the execution of such affairs; or
  - the purpose of use is evident from the circumstances around the collection of the personal information.

The Ministry of Economy, Trade and Industry Guidelines Targeting the Economic and Industrial Sectors Pertaining to the Protection of Personal Information include examples of how business operators can make such public announcement – namely, by posting it on their websites or displaying it in an easily viewable location within their places of business.

Once amended, the Act on the Protection of Personal Information will provide that – as a general rule – business operators must not obtain ‘sensitive information’ without the individual’s prior consent. Details of such information will be specified in a cabinet order.

**Storage**

Business operators governed by the Act on the Protection of Personal Information must take security control measures in regards to personal data. The act imposes a broadly stated obligation on business operators to “take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the Personal Data”. The act provides no concrete measures to satisfy this requirement. However, it is generally understood that such security control measures include:

- organisational measures;
- employee-related measures (eg, personnel training);
- physical measures; and
- technical measures.

Specific actions to be taken for each type of measure are stipulated in the various ministry guidelines.

**Are there any limitations or restrictions on the period for which an organisation may (or must) retain records?**

There are no limitations or restrictions regarding the retention period for personal data.

Once amended, the Act on the Protection of Personal Information will provide that – as a general rule – business operators governed by the act must endeavour to delete personal data without delay when its use is no longer required.

**Do individuals have a right to access personal information about them that is held by an organisation?**

A business operator governed by the Act on the Protection of Personal Information must make the following details accessible to individuals whose personal data it retains:

- its name;
- the purpose of use (except in specified circumstances);
- the procedures for requesting correction, cessation of use, sharing or deletion of the retained personal data, as well as the procedures for other requests; and
other matters as specified by cabinet order that are necessary to ensure the proper handling of the retained personal data.

In addition, business operators governed by the act must disclose any relevant personal data without delay if:

- an individual requests that the business operator disclose whether it has retained any personal data that could lead to the individual's identification; or
- an individual requests notification that the business operator holds no such personal data.

Do individuals have a right to request deletion of their data?

If an individual requests that a business operator governed by the Act on the Protection of Personal Information correct, expand or delete his or her retained personal data because it is inaccurate, the business operator must investigate the issue without delay. Based on the investigation results, the business operator must correct, expand or delete the personal data and notify the individual of its response to the request.

In addition, if an individual requests that a business operator stop using or disclosing retained personal data on the basis that it is violating the Act on the Protection of Personal Information, the business operator must stop using or disclosing the personal data if the request is reasonable.

Consent obligations

Is consent required before processing personal data?

As a general rule, business operators governed by the Act on the Protection of Personal Information cannot handle personal information for reasons beyond the scope necessary to achieve the purpose of use without obtaining the individual’s prior consent.

As a general rule, business operators governed by the act may not provide such information to a third party without obtaining the individual's prior opt-in consent.

If consent is not provided, are there other circumstances in which data processing is permitted?

Exceptions to the general rules above apply if:

- the handling of personal information is required by laws and regulations;
- the handling of personal information is necessary to protect an individual’s life, body or property and obtaining his or her consent would be difficult;
- the handling of personal information is necessary to improve public health or promote the positive growth of children and obtaining the individual’s consent would be difficult; or
- cooperation with a state agency, local government or third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and obtaining the individual’s consent would likely impede the execution of such affairs.

What information must be provided to individuals when personal data is collected?

As a general rule, once a business operator governed by the Act on the Protection of Personal Information has acquired personal information, it must notify the individual of or publicly announce the purpose of use.
Data security and breach notification

Security obligations

Are there specific security obligations that must be complied with?

Business operators governed by the Act on the Protection of Personal Information have a broad obligation to “take necessary and proper measures for the prevention of leakage, loss, or damage, and for other security control of the Personal Data”.

Breach notification

Are data owners/processors required to notify individuals in the event of a breach?

Notifying individuals when a security breach has occurred is not required under the Act on the Protection of Personal Information, but it is mentioned in some guidelines. For example, while the Ministry of Economy, Trade and Industry Guidelines Targeting the Economic and Industrial Sectors Pertaining to the Protection of Personal Information include no express provisions imposing such an obligation, they provide that “it is preferable to apologize to the person for the accident or violation, and to contact the person, as much as possible, in order to prevent secondary damage”. They also include an example of security control measures that should be taken to secure personal information under the act.

Are data owners/processors required to notify the regulator in the event of a breach?

While this is not required under the Act on the Protection of Personal Information, some guidelines require or recommend that the relevant minister be notified. For example, the Financial Services Agency (FSA) Guidelines Targeting Financial Sectors Pertaining to the Protection of Personal Information state that if a personal information breach occurs, the business operator handling the personal information should immediately report the breach to the FSA and promptly make a public announcement addressing – among other things – the facts around the breach and the measures to be taken to prevent a recurrence.

Electronic marketing and internet use

Electronic marketing

Are there rules specifically governing unsolicited electronic marketing (spam)?

The Act on Specified Commercial Transactions (57/1975) prohibits companies from advertising their sales terms by email without the customer’s prior request or consent. Further, the Act on the Regulation of Transmission of Specified Electronic Mail (26/2002) regulates the transmission of emails as a means of advertisement of sales activities. Under this act, in principle companies must not transmit such emails without the customer’s prior request or consent.

Therefore, sending unsolicited email marketing messages (ie, spam) is prohibited by the Act on Specified Commercial Transactions and the Act on the Regulation of Transmission of Specified Electronic Mail.
Data transfer and third parties

Cross-border data transfer

**What rules govern the transfer of data outside your jurisdiction?**

The Act on the Protection of Personal Information does not restrict the transfer of data outside Japan.

The amended act will restrict the provision of personal information to third parties (excluding those operators with a management system conforming to the standards set out in the Personal Information Protection Commission (PPC) rules) in a foreign country (excluding countries that are specified in the PPC rules as having a system for the protection of personal information to that required under Japanese law) without the individual’s prior consent.

**Are there restrictions on the geographic transfer of data?**

The Act on the Protection of Personal Information and most guidelines include no restrictions on the geographic transfer of data. However, the guidelines regarding medical information systems provide that medical information systems (eg, servers including medical information) and medical data should be located in an area where Japanese laws can be enforced.

Third parties

**Do any specific requirements apply to data owners where personal data is transferred to a third party for processing?**

As a general rule, business operators governed by the Act on the Protection of Personal Information cannot provide personal information to a third party without obtaining the individual’s prior opt-in consent.

The amended act will require business operators providing personal data to third parties to record:

- the date on which the data was provided;
- the third party’s name; and
- the matters specified in the PPC rules.

Conversely, if a business operator receives such personal data from a third party, it must confirm:

- the third party’s name and address;
- the representative’s name; and
- how the third party obtained the personal data.

In addition, the business operator must record the date on which the information was provided and any matters regarding such confirmation, as well as the matters specified by the PPC rules.

**Exceptions**
Exceptions to the general rule above apply if:

- the handling of personal data is required under laws and regulations;
- the handling of personal data is necessary for the protection of the individual’s life, body or property and obtaining his or her consent would be difficult;
- the handling of personal data is necessary to improve public health or promote the positive growth of children and obtaining the individual’s consent would be difficult; and
- cooperation with a state agency, local government or third party commissioned by a state or local agency is necessary to conduct certain affairs specified by laws and regulations and obtaining the individual’s consent would likely impede the execution of such affairs.

The following exceptions also apply:

- A business operator governed by the Act on the Protection of Personal Information can provide personal data to a third party without obtaining the individual’s prior consent if it notifies the individual in advance of the following information or makes such information readily available to the individual:
  - the fact that providing the personal data to a third party falls under the purpose of use;
  - the personal data that will be provided to the third party;
  - the means or methods of providing the personal data to the third party; and
  - the fact that the provision of the personal data – which will lead to the identification of the individual by a third party – will be discontinued on the individual’s request to opt out.

Once amended, the Act on the Protection of Personal Information will also require business operators to advise on the way in which an individual can make an opt-out request and to notify the PPC of all of the above information. They will also be prohibited from providing sensitive information to third parties by using the opt-out option.

- If the personal data is to be transferred as a result of a merger, acquisition or similar succession transaction, the recipient does not constitute a third party.
- If the personal data is to be transferred as a result of a third-party service provider’s commissioning of a business operator for all or part of the processing of the personal data that is necessary to achieve the purpose of use, and the service provider does not process the data for its own purpose of use, such service provider does not constitute a third party.
- A business operator governed by the Act on the Protection of Personal Information can use the personal information jointly with another individual or entity without the individual’s prior consent if it notifies the individual of the following information or ensures that such information is made readily available to the individual, in advance:
  - the fact that the personal data may be shared with and used jointly by specific individuals or entities;
  - the personal data that will be jointly used;
  - the scope of the joint users;
  - the purpose for which the personal data will be used; and
  - the name of the joint user responsible for the management of the personal data (either an individual or a business operator).

Penalties and compensation

**Penalties**

What are the potential penalties for non-compliance with data protection provisions?

Under the Act on the Protection of Personal Information, ministries may request reports on the handling of personal information and may issue recommendations or corrective orders if a business operator governed by the act breaches an individual’s privacy and violates the act.

Before issuing a corrective order, ministries may take an incremental approach and instruct, advise and make recommendations to business operators governed by the act. A breach of a corrective order is a criminal offence and the person responsible is punishable by imprisonment with work for a maximum of six months, a maximum fine of ¥300,000 or both. The business operator will also be subject to a maximum fine of ¥300,000.

**Compensation**

Are individuals entitled to compensation for loss suffered as a result of a data breach or non-compliance with
If an individual’s privacy is violated due to a business operator governed by the act’s data breach or non-compliance with data protection provisions, the individual may file a tort or breach of contract claim for compensation against the business operator.

Cybersecurity

Has legislation been introduced in your jurisdiction that specifically covers cybercrime and/or cybersecurity?

Several laws cover different types of cybercrime and cybersecurity, such as:

- the Penal Code (45/1907), which was amended in 2011 to regulate ‘illegal programming’, including malware (Articles 168-2 and 168-3);
- the Act on the Prohibition of Unauthorised Computer Access (128/1999), which was enacted in 1999 and amended in 2012 to include phishing and the unauthorised obtainment of identifying information (eg, passwords); and
- the Unfair Competition Prevention Act (47/1993), which prohibits unauthorised access to trade secrets and was amended in 2015 to strengthen penalties.

What are the other significant regulatory considerations regarding cybersecurity in your jurisdiction (including any international standards that have been adopted)?

The Basic Act on Cybersecurity (104/2014) was enacted in November 2014 to promote and enhance cybersecurity in Japan. The act sets out an overall national cybersecurity policy and the roles and responsibilities of the national and local governments. The act also provides that cyber businesses and infrastructure-related businesses should endeavour to take voluntary measures to enhance cybersecurity and cooperate with the government in implementing the relevant measures (Article 7).

Which cyber activities are criminalised in your jurisdiction?

The following cyber activities are criminalised in Japan, among others:

- the creation, provision, release, acquisition and storage of malware with the intention of applying or using such malware in the electronic device of another person or entity (Articles 168-2 and 168-3 of the Penal Code);
- phishing and the unauthorised obtainment of identifying information (eg, passwords and fingerprint data) via online access (Articles 2, 3, 4 and 7 of the Act on the Prohibition of Unauthorised Computer Access);
- Unauthorised online access of computer systems or networks (Articles 2 and 3 of the Act on the Prohibition of Unauthorised Computer Access); and
- the unauthorised acquisition, use or disclosure of trade secrets (including those that are electronically stored) in a physical or electronic manner with the intention of acquiring an illicit gain or causing injury to the owner (Article 2 of the Unfair Competition Prevention Act).

Which authorities are responsible for enforcing cybersecurity rules?
The Basic Act on Cybersecurity designates the Cybersecurity Strategic Headquarters as the control body to promote national cybersecurity strategy and the National Centre of Incident Readiness and Strategy for Cybersecurity as its secretariat.

With respect to cybercrime, the National Police Agency and the Prosecutor’s Office are responsible for enforcing the applicable laws.

Cybersecurity best practice and reporting

Can companies obtain insurance for cybersecurity breaches and is it common to do so?

Yes, but it is uncommon, especially for small and medium-sized companies.

Are companies required to keep records of cybercrime threats, attacks and breaches?

There is no such legal obligation. However, the Act on the Prohibition of Unauthorised Computer Access provides that an administrator of computer systems or networks should endeavour to consistently check the integrity of its access control functions (Article 8). Therefore, it can be construed that companies endeavour to keep such records in order to properly control their computer systems.

Are companies required to report cybercrime threats, attacks and breaches to the relevant authorities?

There is no such legal obligation. If cybercrime entails a personal data breach, the company will be required to report it to the competent minister in accordance with the applicable guidelines.

Are companies required to report cybercrime threats, attacks and breaches publicly?

There is no such legal obligation. If cybercrime entails a personal data breach, the company will be required to report it to the individuals concerned in accordance with the applicable guidelines.

Criminal sanctions and penalties

What are the potential criminal sanctions for cybercrime?

Criminal sanctions for the major types of cybercrime in Japan are as follows:

- The creation, provision or release of malware can result in imprisonment with work for a maximum of three years or a maximum fine of Y500,000 (Article 168-2 of the Penal Code).
- The acquisition or storage of malware can result in imprisonment with work for a maximum of two years or a maximum fine of Y300,000 (Article 168-3 of the Penal Code).
- Phishing and the unauthorised obtainment of identifying information via an online system can result in imprisonment...
What penalties may be imposed for failure to comply with cybersecurity regulations?

There are no such penalties. However, if such failure also falls under non-compliance with data protection provisions, the relevant minister may issue recommendations and corrective orders and a breach of such corrective orders is a criminal offence.

Law stated date

Correct as of

Please state the date of which the law stated here is accurate.

June 2016.