DATA PROTECTION & PRIVACY

Japan

LEXOLOGY
Getting The Deal Through

Consulting editor
Hunton Andrews Kurth LLP

Data Protection & Privacy

Consulting editors

Aaron P Simpson, Lisa J Sotto

Hunton Andrews Kurth LLP

Quick reference guide enabling side-by-side comparison of local insights into the legislative framework; relevant authorities; treatment of breaches; legitimate processing; data handling responsibilities of PII owners; security obligations; internal controls, including the data protection officer; registration formalities transfer and disclosure of PII; rights of individuals; judicial supervision; specific data processing use cases such as cookies, electronic communications marketing, and cloud services; and recent trends.

Generated 17 July 2023

Table of contents

Contributors

Japan

Masaki Mizukoshi
masaki_mizukoshi@noandt.com
Nagashima Ohno & Tsunematsu

NAGASHIMA OHNO & TSUNEMATSU

Saaya Shiina
saaya_shiina@noandt.com
Nagashima Ohno & Tsunematsu

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The Act on the Protection of Personal Information of 2003, as amended (APPI), sits at the centre of Japan's regime for the protection of personal information (PI). Serving as a comprehensive, cross-sectoral framework, the APPI regulates both private businesses using PI databases and the governmental sector and is generally considered to embody the eight basic principles under the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The APPI is implemented by cross-sectoral administrative guidelines prepared by the Personal Information Protection Commission (the Commission). In relation to certain sectors, such as medical, financial and telecommunications, the Commission and the relevant government ministries have published sector-specific guidance providing for additional requirements given the highly sensitive nature of PI handled by private business operators in those sectors. Numerous self-regulatory organisations and industry associations have also adopted their own policies or guidelines for the protection of PI.

The APPI has undergone several significant amendments. One of the recent significant amendments was promulgated on 12 June 2020 (the 2020 Amendment) and fully implemented on 1 April 2022. The 2020 Amendment includes, inter alia, a statutory obligation to report certain data breaches to the Commission and notify affected individuals of data breaches that are likely to cause the violation of individual rights and interests.

Another recent amendment was promulgated on 19 May 2021 (the 2021 Amendment) and fully implemented on 1 April 2023, which expanded the scope of the APPI to include rules applicable not only to private sectors but also to governmental sectors.

Law stated - 31 May 2023

Data protection authority

Which authority is responsible for overseeing the data protection law? What is the extent of its investigative powers?

The Commission was established on 1 January 2016 as a cross-sectoral, independent government body to oversee the APPI. The Commission has the authority, based on the APPI, to monitor and supervise private business operators handling PI and to monitor the administrative governmental sector. For example, the Commission has the following powers over private business operators handling PI under the APPI:

- to require reports concerning the handling of PI, pseudonymised information, anonymised information or individual-related information from private business operators using 'databases, etc' of PI (PI databases), pseudonymised information (pseudonymised information databases), anonymised information (anonymised information databases) or individual-related information (individual-related information databases);
- to conduct an on-site inspection of offices or other premises of private business operators to raise questions and inspect records concerning their handling of PI, pseudonymised information, anonymised information or individual-related information;

- to give 'guidance' or 'advice' necessary for the handling of PI, pseudonymised information, anonymised information or individual-related information to private business operators using PI databases, pseudonymised information databases, anonymised information databases or individual-related information databases;
- upon violation of certain obligations of any private business operator using PI databases, pseudonymised information databases, anonymised information databases or individual-related information databases and to the extent deemed necessary to protect the rights of an affected individual, to 'recommend' cessation or other measures necessary to rectify the violation; and
- if recommended measures are not implemented and the Commission deems an imminent danger to the affected individual's material rights, to order such measures.

The Commission may delegate the power to require reports or conduct an on-site inspection to certain government ministries in cases where the Commission deems it necessary to be able to give guidance or advice effectively. The Commission is also empowered to require reports from, conduct on-site inspections for and order measures against foreign private business operators that are subject to the APPI, signalling the broader extraterritorial application of the APPI.

Law stated - 31 May 2023

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Under the APPI, in cases where government ministries deem it necessary to ensure the proper handling of PI, such government ministries may request the Commission to take appropriate measures following the provisions of the APPI.

Also, under the APPI, the Commission may provide foreign authorities enforcing foreign laws and regulations equivalent to the APPI with information that the Commission deems beneficial to the duties of such foreign authorities that are equivalent to the Commission's duties outlined in the APPI. Upon request from the foreign authorities, the Commission may consent that the information provided by it be used for an investigation of a foreign criminal case, subject to certain exceptions.

Law stated - 31 May 2023

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under the APPI, criminal penalties may be imposed if there has been:

- failure to comply with any order issued by the Commission (subject to penal servitude of up to one year or a criminal fine of up to ¥1,000,000);
- failure to submit reports, or submitting of untrue reports, as required by the Commission (subject to a criminal fine of up to ¥500,000);
- refusal or interruption of an on-site inspection of the offices or other premises by the Commission (subject to a criminal fine of up to ¥500,000); or
- theft or provision to a third party by any current or former officer, employee or representative of a private business operator of information from a PI database he or she handled in connection with the business of the private

business operator for the purpose of seeking unlawful benefits to himself or herself or third parties (subject to penal servitude of up to one year or a criminal fine of up to ¥500,000).

If the foregoing offences are committed by an officer or employee of a subject private business operator that is a judicial entity, then the entity itself may also be held liable for a criminal fine. The amount of the criminal fine for the judicial entity is up to ¥100 million for the offences outlined in the first and last bullet points, and up to ¥500,000 for the offences outlined in the second and third bullet points.

Law stated - 31 May 2023

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Administrative law in Japan usually provides for an appeal of a government ministry's decision to a court with proper jurisdiction. Therefore, if the Commission or the relevant government ministry to which powers of the Commission are duly delegated takes administrative actions against a private business operator using PI databases, it will generally be able to challenge the actions judicially.

Law stated - 31 May 2023

SCOPE

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Act on the Protection of Personal Information of 2003, as amended (APPI) contains notable exemptions for private sectors, as follows:

- In respect of fundamental constitutional rights, media outlets and journalists, religious groups and political parties are exempt from the APPI to the extent of the processing of personal data for purposes of journalism, and religious and political activities, respectively.
- The use of personal information (PI) for personal purposes is outside the scope of the APPI. The use of PI by not-for-profit organisations or sole proprietorships is within the scope of the APPI.

As for government sectors, there are exemptions to the rights of individuals, such as the right to disclosure, correction and suspension of use of PI concerning criminal cases or the like.

Law stated - 31 May 2023

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

Secrecy of communications from the government’s intrusion is a constitutional right. Interception of electronic communication by private persons is regulated by the Telecommunications Business Act of 1984 and the Act on the

Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders of 2001. Marketing emails are restricted under the Act on Regulation of Transmission of Specified Electronic Mail of 2002 and the Act on Specified Commercial Transactions of 1976.

Law stated - 31 May 2023

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

The Act on Utilisation of Numbers to Identify Specific Individuals in Administrative Process, amended in April 2023, provides rules concerning the use of PI acquired through the use of the individual social security and tax numbering system, My Number.

In addition, the Act on Anonymously Processed Medical Information to Contribute to Research and Development in the Medical Field, which stipulates regulations on the handling of medical information and anonymously processed medical information, etc, has been enacted as a special law of the APPI and was amended in May 2023.

Law stated - 31 May 2023

PI formats

What categories and types of PI are covered by the law?

The APPI covers PI made part of 'databases, etc' of PI (PI databases). 'PI databases' include electronic databases and manual filing systems that are structured by reference to certain classification criteria so that information on specific individuals is easily searchable.

For purposes of the APPI, 'PI' is defined as information related to a living individual that can identify the specific individual by name, date of birth or other description contained in such information. Information that, by itself, is not personally identifiable but may be easily linked to other information and thereby can be used to identify a specific individual is also regarded as PI. PI also includes signs, code or data that identify physical features of specific individuals, such as fingerprint or face recognition data, or that are assigned to each individual by government or providers of goods or services, such as a driving licence number or passport number. PI comprising a PI database is called personal data.

The APPI provides for three types of data that are distinguished from PI. First, 'anonymised information' means information relating to a particular individual that has been irreversibly processed by applying designated methods for anonymisation such that the individual is no longer identifiable and cannot be reidentified. Anonymised information is not considered PI, and may be disclosed to third parties without the consent of the relevant individual, provided that the business operator who processes and discloses anonymised information to third parties comply with certain disclosure requirements.

Second, 'pseudonymised information' means information relating to a particular individual that has been processed by erasing or replacing all or part of identifiers in such a manner that the individual is no longer identifiable unless it is collated with other information. In most cases, pseudonymised information is considered PI. The pseudonymised information may be used for data analysis or other internal use by operators, but it may not be disclosed to third parties except in certain cases.

Third, 'individual-related information' is a concept newly introduced to impose certain additional obligations relating to

a transfer of information that is not personally identifiable at the transferor but the transferee can identify the relevant individual by linking such information held by the transferee or otherwise. If a transferor anticipates that the transferee can identify the relevant individual of the data being transferred, the transferor must confirm that the transferee has obtained consent from the relevant individual about the transfer.

Law stated - 31 May 2023

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

The APPI has an extraterritorial application. Specifically, the APPI applies to foreign private business operators using PI databases, individual-related information databases, pseudonymised information databases or anonymised information databases when they use or process, outside of Japan, in connection with providing goods or services to individuals in Japan:

- the PI of individuals residing in Japan; or
- individual-related information to be obtained as such PI, or pseudonymised information or anonymised information produced by such private business operators based on such PI.

Separately, the PI of individuals residing outside of Japan is considered to be protected under the APPI as long as such PI is held by private business operators established or operating in Japan.

Law stated - 31 May 2023

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The APPI distinguishes between:

- obligations imposed on private business operators using PI databases (personal data users); and
- obligations imposed only on those private business operators using PI databases who control the relevant personal data (PI data owners).

Generally, service providers are subject to the obligations of personal data users but not subject to the obligations of PI data owners.

The obligations of all personal data users, as mentioned in the first bullet point above, include:

- to specify the purposes for which the PI is used as explicitly as possible;
- to process the PI only to the extent necessary for achieving such specified purposes unless the relevant individual's prior consent is obtained, subject to limited exceptions;
- to notify the relevant individual of, or publicise, the purposes of use before or at the time of collecting PI unless such purposes were publicised before the collection of the PI;

- not to use PI in a manner that potentially facilitates illegal or unjustifiable conduct;
- not to use deceptive or wrongful means in collecting PI;
- to obtain the consent of the individual before collecting sensitive personal information, which includes race, beliefs, social status, medical history, criminal records and the fact of having been a victim of a crime and disabilities (subject to certain exceptions);
- to endeavour to keep its personal data accurate and up to date to the extent necessary for the purposes of use, and erase, without delay, its personal data that is no longer needed to be used;
- to undertake necessary and appropriate measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the personal data it holds;
- to conduct necessary and appropriate supervision over its employees and its service providers who process its personal data;
- to report to the Personal Information Protection Commission and notify a relevant individual when there is data breach that is likely to harm an individual's rights and interests;
- not to disclose the personal data to any third party without the consent of the individual (subject to certain exemptions);
- to prepare and keep records of third-party transfers of personal data (subject to certain exceptions) (as a result of the 2020 Amendment, including to disclose such records upon the individuals' request, subject to certain exceptions);
- when acquiring personal data from a third party other than data subjects (subject to certain exceptions), to verify the name of the third party and how the third party acquired such personal data; and
- not to conduct cross-border transfers of personal data without the consent of the individual (subject to certain exceptions).

The PI data owners mentioned in (2) have additional and more stringent obligations, which are imposed only in respect to personal data for which a PI data owner has the right to provide a copy of, modify (ie, correct, add or delete), discontinue using, erase and discontinue disclosing to third parties (retained personal data):

- to make accessible to the relevant individual certain information regarding the retained personal data, including:
  - the name and address and, for a corporate body, the name of the representative of the PI data owner;
  - all purposes for which retained personal data held by the PI data owner is generally used;
  - procedures for submitting a request or filing complaints to the PI data owner; and
  - security control measures taken by the PI data owner;
- to provide, without delay, a copy of retained personal data to the relevant individual upon his or her request (subject to certain exceptions);
- to correct, add or delete the retained personal data to the extent necessary for achieving the purposes of use upon the request of the relevant individual (subject to certain exceptions);
- to discontinue the use of or erase such retained personal data upon the request of the relevant individual if such use is or was made, or the retained personal data in question was obtained, in violation of the APPI or if it has become unnecessary to use such retained personal data, a data breach has occurred in connection with such retained personal data, or there is a possibility that handling of such retained personal data would harm the rights or legitimate interests of the relevant individual (subject to certain exceptions); and
- to discontinue disclosure of retained personal data to third parties upon the request of the relevant individual if such disclosure is or was made in violation of the APPI or if it has become unnecessary to use such retained personal data, a data breach has occurred in connection with such retained personal data, or there is a possibility that handling of such retained personal data would harm the rights or legitimate interests of the relevant individual (subject to certain exceptions).

Under the APPI, any personal data where the existence or absence of such personal data would harm the life, body and property of the relevant individual or a third party; encourage or solicit illegal or unjust acts; jeopardise the safety of Japan and harm the trust or negotiations with other countries or international organisations; or impede criminal investigations or public safety is excluded from the retained personal data and therefore does not trigger the above-mentioned obligations of PI data owners.

Law stated - 31 May 2023

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

The Act on the Protection of Personal Information of 2003, as amended (APPI), does not contain specific criteria for legitimate data collection or processing. The APPI does, however, prohibit the collection of personal information (PI) by deceptive or wrongful means, and requires that the purposes of use must be identified as specifically as possible, and must generally be notified or made available to the relevant individual in advance. In addition, the APPI provides that PI should not be used in a manner that potentially facilitates illegal or unjustifiable conduct. Further, processing of PI beyond the extent necessary for such purposes of use without the relevant individual's prior consent is also prohibited, subject to limited exceptions.

Law stated - 31 May 2023

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

The APPI imposes stringent rules for sensitive personal information, including race, beliefs, social status, medical history, disabilities, criminal records and the fact of having been a victim of a crime. Collection or disclosure under the 'opt-out' mechanism of sensitive personal information without the consent of the relevant individual is generally prohibited.

Also, the administrative guidelines for the financial sector provide for a similar category of sensitive information. Such information is considered to include trade union membership, domicile of birth and sexual orientation, in addition to sensitive personal information. The collection, processing or transfer of such sensitive information by financial institutions is prohibited, even with the consent of the relevant individual, except under limited circumstances permitted under such administrative guidelines.

Further, in January 2019, upon the decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the EU's General Data Protection Regulation (GDPR), the supplementary rules regarding the handling of personal data transferred from the European Economic Area (EEA) based on an adequacy decision by the European Commission (the EEA Data Supplementary Rules) have taken effect. The EEA Data Supplementary Rules impose stringent rules for the personal data transferred from the European Economic Area based on an adequacy decision by the European Commission (EEA data). Upon Brexit, the effect of the adequacy decision by the European Commission has been sustained in the United Kingdom; therefore, EEA data includes the personal data transferred from the United Kingdom and the reference to 'EEA' includes the United Kingdom in this chapter. The mutual adequacy arrangement was subject to a first review, which has been concluded with the adoption of reports by the Personal Information Protection Commission and the European Commission on the functioning of their respective

adequacy decisions. This review has made it mutually clear that an adequate level of protection of personal data continues to be ensured. The Supplementary Rules, amended as a result of the review, can be summarised as follows:

- In cases where EEA data includes data concerning sex life, sexual orientation or trade union membership it is categorised as a special category of personal data under the GDPR, such EEA data is treated as 'sensitive personal information' under the APPI.
- When a private business operator using PI databases receives EEA data from the EEA, the private business operator is required to confirm and record the purposes of use of such EEA data specified at the time of acquisition from the relevant data subject (original purposes of use).
- When a private business operator using PI databases receives EEA data from another private business operator who received such EEA data from the EEA, the first private business operator is also required to confirm and record the original purposes of use of such EEA data.
- In each case of the second and third bullet points above, the private business operator must specify the purposes of use of EEA data within the scope of the original purposes of use of such EEA data, and use such EEA data following such specified purposes of use.
- When a private business operator using PI databases processes EEA data to create anonymised information under the APPI, the private business operator is required to delete any information that could be used to re-identify the relevant individuals, including any information concerning the method of the process for anonymisation.
- In cases where a private business operator using PI databases proposes to transfer EEA data it received from the EEA on to a third party transferee located outside of Japan (ie, onward transfer), the private business operator must:
  - provide the data subjects of such EEA data with information concerning the transferee, and obtain prior consent to the proposed cross-border transfer from the data subject; or
  - transfer relying on applicable exemptions of such cross-border transfer.
- Pseudonymised information obtained by processing EEA data from the EEA must be treated in accordance with the rules applicable to pseudonymised information that constitutes PI and must be processed only for statistical purposes.

Law stated - 31 May 2023

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

There are several notification requirements under the Act on the Protection of Personal Information of 2003, as amended (APPI).

First, the APPI requires all personal data users to notify individuals of, or make available to individuals, the purpose for which their personal information (PI) is used, promptly after the collection of the PI, unless the purpose was publicised before the collection of the PI. Alternatively, such purpose must be expressly stated in writing if collecting PI provided in writing by the individual directly.

Second, when a private business operator using PI databases is to disclose personal data to third parties without the individual's consent under the 'opt-out' mechanism, one of the requirements that the private business operator must satisfy is that certain information regarding the third-party disclosure is notified, or made easily accessible, to the individual before such disclosure. Such information includes the types of information being disclosed and the manner

of disclosure.

Third, when a private business operator using PI databases is to disclose personal data to third parties without the individual's consent under the 'joint-use' arrangement, the private business operator must notify or make easily accessible, certain information regarding the third-party disclosure before such disclosure. Such information includes items of personal data to be jointly used, the scope of third parties who would jointly use the personal data, the purpose of use by such third parties, and the name and address and, for a corporate body, the name of the representative of a party responsible for the control of the personal data in question.

Fourth, the APPI requires each PI data owner to keep certain information accessible to those individuals whose retained personal data is held. Such information includes:

- the name and address and, for a corporate body, the name of the representative of the PI data owner;
- all purposes for which retained personal data held by the PI data owner is generally used;
- the procedures for submitting a request or filing complaints to the PI data owner; and
- security control measures taken by the PI data owner.

If, based on such information, an individual requests the specific purposes of use of his or her retained personal data, the PI data owner is required to notify, without delay, the individual of such purposes.

Fifth, without delay after having prepared anonymised information, a private business operator must disclose, through the Internet or other appropriate measures, the categories of information on an individual to whom the anonymised information pertains.

Law stated - 31 May 2023

Exemptions from transparency obligations

When is notice not required?

There is an exception to the notice requirement imposed on a private business operator using PI databases when collecting PI where among other circumstances:

- such notice would harm the interest of the individual or a third party;
- such notice would harm the legitimate interest of the private business operator; and
- the purposes of use are evident from the context of the collection of the relevant personal data.

Law stated - 31 May 2023

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

The APPI requires all private business operators using PI databases to endeavour to:

- keep the personal data they hold accurate and up to date to the extent necessary for the purposes for which the personal data is to be used; and
- erase, without delay, such personal data that is no longer needed.

As a result of the 2020 Amendment, PI data owners must, upon the relevant individual's request, discontinue the use of or erase retained personal data that is no longer needed.

Law stated - 31 May 2023

Data minimisation

Does the law restrict the types or volume of PI that may be collected?

The APPI does not restrict the types or volume of PI that may be collected, other than restricting the collection of sensitive personal information without obtaining the consent of the relevant individual. Sensitive personal information includes information on race, beliefs, social status, medical history, disabilities, criminal record and the fact of having been a victim of a crime.

Law stated - 31 May 2023

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

No. Personal data may be held as long as is necessary for the purposes for which it was collected. Under the APPI, private business operators using PI databases must endeavour to erase, without delay, such personal data that no longer needs to be used.

In addition, as a result of the 2020 Amendment, such private business operators must, upon the relevant individual's request, discontinue the use of or erase retained personal data that is no longer needed.

Law stated - 31 May 2023

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI can generally be used only to the extent necessary to achieve such specified purposes as notified or made available to the relevant individual. Use beyond such extent or for any other purpose must, in principle, be legitimised by the consent of the relevant individual.

Exemptions from the purposes for use requirement apply to, for instance, the use of PI pursuant to laws, and where use beyond specified purposes is needed to protect life, body and property of a person and it is difficult to obtain the consent of the affected individual.

In addition, under the APPI, the purpose for use may be amended, without the consent of the relevant individual, to the limited extent that would be reasonably deemed to be related to the previous purposes.

PI may be used for such amended purposes, provided that the amended purposes are notified or made available to the affected individuals.

Law stated - 31 May 2023

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

The APPI does not restrict the use of PI for automated decision-making, and PI can generally be used to the extent necessary to achieve such specified purposes as notified or made available to the relevant individual.

However, the APPI requires that the purpose of use should be specified as explicitly as possible. In this regard, the Personal Information Protection Commission explains in one of its cross-sectoral administrative guidelines for the APPI that when analysing information, such as behaviours and interests related to an individual from the information obtained from the individual, private business operators using PI databases must specify the purpose of the use to the extent that such individual can predict and assume what kind of processing will be performed.

Law stated - 31 May 2023

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

The Act on the Protection of Personal Information of 2003, as amended (APPI) provides that all personal data users must have in place 'necessary and appropriate' measures to safeguard and protect against unauthorised disclosure of or loss of or damage to the personal data they hold or process; and conduct necessary and appropriate supervision over their employees and service providers who process such personal data. What constitutes 'necessary and appropriate' security measures is elaborated on in the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines). The Commission Guidelines set forth a long list of four types of mandatory or recommended security measures – organisational, personnel, physical and technical – as well as the requirement to adopt internal security rules or policies. The Commission Guidelines also require that, when private business operators using personal information (PI) databases handle personal data in a foreign country, they must take necessary and appropriate measures for the security control of personal data after understanding the PI protection regime of such foreign country.

In addition, some of the sector-specific guidelines, such as the administrative guidelines for the financial sector, provide for more stringent requirements on security measures.

Law stated - 31 May 2023

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Under the APPI, private business operators are required to report to the Personal Information Protection Commission (the Commission) and notify affected individuals of a data breach that is highly likely to harm the rights and interests of affected individuals. A leakage, loss or damage of personal data constitutes such a data breach.

The enforcement rules provide that such reporting obligation will be triggered if:

- a data breach of sensitive personal information has occurred or is likely to have occurred;
- a data breach that may cause financial damage due to unauthorised use has occurred, or is likely to have occurred;
- a data breach that may have been committed with a wrongful purpose has occurred or is likely to have occurred; and
- a data breach where more than 1,000 data subjects have been or are likely to be affected.

As for reporting to the Commission, a business operator will be required to make both 'prompt reporting' and 'confirmatory reporting.' When becoming aware of a data breach of any of the categories mentioned above, a business operator must 'promptly' report to the Commission based on its knowledge of the data incident at that time. The 'promptly' is construed to approximately be three to five days. Subsequently, the business operator must make confirmatory reporting within 30 days (or 60 days if the data breach may have been committed for a wrongful purpose).

As for notification to affected data subjects, the enforcement rules require that the business operator notify them 'promptly in light of the relevant circumstances'. Unlike the obligation to report to the Commission, the business operator may be exempted from so notifying if it is difficult to notify them and sufficient alternative measures are taken to protect their rights and interests.

Law stated - 31 May 2023

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

Under the Act on the Protection of Personal Information of 2003, as amended (APPI), private business operators using personal information (PI) databases (regardless of whether they are owners or processors of PI) are obliged to take necessary and appropriate measures for the security control of personal data. According to the Personal Information Protection Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines), such necessary and appropriate measures include the following:

- to establish basic policies that declare the stance of the private business operator towards taking necessary and appropriate measures for the control of personal data;
- to establish internal rules with respect to the handling of personal data;
- to implement organisational, personal, physical and technical control measures; and
- to take necessary and appropriate measures for the control of personal data after understanding the PI protection regime of a foreign country, when handling personal data in such a foreign country.

Law stated - 31 May 2023

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no statutory requirement to appoint a data protection officer. However, the appointment of a 'chief privacy officer' is generally recommended under the Commission Guidelines. The Commission Guidelines do not provide for the qualifications, roles or responsibilities of a chief privacy officer.

Law stated - 31 May 2023

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Under the APPI, private business operators using PI databases that have disclosed personal data to third parties must generally keep records of such disclosure. Also, private business operators receiving personal data from third parties rather than the relevant individuals must generally verify how the personal data was acquired by such third parties and keep records of such verification.

The foregoing obligation does not apply to the disclosure of personal data to outsourced processing service providers, as part of mergers and acquisitions transactions or for joint use, as long as the disclosure is not based on consent regarding the cross-border transfer restrictions.

Law stated - 31 May 2023

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

The APPI does not oblige private business operators using PI databases (regardless of whether they are owners or processors of PI) to carry out risk assessments in relation to the use of PI.

However, the APPI requires private business operators to take necessary and appropriate measures for the security control of personal data as well as supervise their employees and outsourced service providers. In this regard, it is recommended under the Commission Guidelines that such appropriate measures and supervision be conducted in accordance with the risks arising from the nature and size of the business, status of use of the PI (including the nature and quantity of PI) and the media on which PI is recorded. Therefore, to implement the appropriate measures for security control, it is expected under the APPI that private business operators will implement risk assessments in connection with such aspects.

Law stated - 31 May 2023

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

No. However, the Commission Guidelines generally require that, when implementing security measures to safeguard the personal data it holds or processes, each private business operator using PI databases should consider the degree of the impact of any unauthorised disclosure or another incident on the right or interest of one or more data subjects affected by such an incident.

Law stated - 31 May 2023

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Under the Act on the Protection of Personal Information of 2003, as amended (APPI), personal data users who disclose personal data (other than certain personal data such as sensitive personal information) under the 'opt-out' mechanism are required to submit a notification to the Personal Information Protection Commission (the Commission) before such disclosure. According to the Commission, the primary target of this requirement is mailing list brokers.

Notification to the Commission regarding the opt-out mechanism should include certain matters, such as the categories of personal data to be disclosed, the method of disclosure, how the relevant individual may request to cancel such opt-out disclosure to the private business operators and other designated matters. No penalties are statutorily provided for the failure to submit notification of such opt-out disclosure.

Law stated - 31 May 2023

Other transparency duties

Are there any other public transparency duties?

Apart from the matters required under the APPI to notify individuals as separately mentioned in this chapter, the Commission Guidelines recommend that private business operators using personal information (PI) databases make public an outline of the processing of personal data such as whether the private business operators outsource the processing of personal data and the contents of the processing to be outsourced.

Also, the administrative guidelines for the financial sector recommend that private business operators using PI databases make public:

- the purpose of the use of PI;
- whether the private business operators outsource the processing of personal data;
- the contents of the processing to be outsourced;
- the sources and methods of obtaining PI; and
- a statement to the effect that upon the request of individuals, the use of retained personal data will be discontinued.

Law stated - 31 May 2023

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

The Act on the Protection of Personal Information of 2003, as amended (APPI) generally prohibits disclosure of personal data to third parties without the relevant individual's consent. As an exception to such prohibition, the transfer of all or part of personal data to persons that provide outsourced processing services is permitted to the extent such services are necessary for achieving the permitted purposes of use. Private business operators using personal

information (PI) databases are required to engage in 'necessary and appropriate' supervision over such service providers to safeguard the transferred personal data. Necessary and appropriate supervision by private business operators is generally considered to include:

- proper selection of service providers;
- entering into a written contract setting forth necessary and appropriate security measures; and
- collecting necessary reports and information from the service providers.

The APPI does not set forth specific contractual obligations that must be included in the above contract. However, in practice, it is desirable for certain matters to be included in the contract, such as matters for the control of personal data, sub-processing, reports from the service providers, confirmation of the compliance of the contract (such as information security auditing), measures in the case of non-compliance with the contract and communications in the case of a data breach.

Law stated - 31 May 2023

Restrictions on third-party disclosure

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

In principle, the APPI prohibits sharing of PI to a third party without the individual's consent. Important exceptions to the general prohibition include the following, in addition to sharing for outsourced processing services, the following restrictions apply.

Disclosure under the 'opt-out' mechanism

A private business operator using PI databases may share personal data with third parties without the individual's consent, provided that:

- it is prepared to cease such sharing upon request from the individual;
- certain information regarding such sharing is notified, or made easily accessible, to the individual before such disclosure; and
- such information is notified to the Personal Information Protection Commission (the Commission) in advance.

Transfer in mergers and acquisitions transactions

Personal data may be transferred without the consent of the individual in connection with the transfer of a business as a result of a merger or other transactions.

Sharing for joint use

A private business operator using PI databases user may disclose personal data it holds to a third party for joint use, provided that certain information regarding such joint use is notified, or made easily accessible, to the individual before such disclosure. Such disclosure is most typically made when sharing customer information among group companies to provide seamless services within the permitted purposes of use. Information required to be notified or made

available includes items of personal data to be jointly used, the scope of third parties who would jointly use the personal data, the purpose of use by such third parties, and the name and address and, for a corporate body, the name of the representative of a party responsible for the control of the personal data in question.

Law stated - 31 May 2023

Cross-border transfer

Is the transfer of PI outside the jurisdiction restricted?

The APPI does not stipulate any supervisory authority notification requirements nor authorisation requirements. Under the APPI, the transfer of personal data to a third party located outside Japan is generally subject to the prior consent of the relevant individual, subject to the important exceptions mentioned below.

First, no prior consent of the relevant individual is required if the third party is located in a foreign country that the Commission considers has the same level of protection of PI as Japan. On 23 January 2019, countries in the European Economic Area were designated as such by the Commission in exchange for the parallel decision by the European Commission that Japan ensures an adequate level of protection of personal data under article 45 of the General Data Protection Regulation. Such designation by the Commission covers the United Kingdom post Brexit.

The second exception is applicable where the relevant third-party transferee has established a system to continuously ensure its undertaking of the same level of protective measures as private business operators using PI databases would be required under the APPI. According to the Commission's cross-sectoral administrative guidelines for the APPI (the Commission Guidelines), for this exception to apply, the private business operator and the foreign third party may ensure in a contract that:

- the third party undertakes such protective measures; and
- if the third party is an intra-group affiliate, the data user and the foreign third party may rely on a privacy statement or internal policies applicable to the group that are appropriately drafted and enforced.

Also, this exception is generally applicable if the foreign third party has certification from an internationally recognised framework of protection of personal data; specifically, certification under the Asia-Pacific Economic Cooperation's Cross Border Privacy Rules system.

In addition, the 2020 Amendment, which fully took effect on 1 April 2022, has imposed enhanced obligations on cross-border transfer. First, when obtaining prior consent to the cross-border transfer from data subjects whose data is to be transferred overseas, the private business operator must provide them with the name of the foreign country where the relevant PI is transferred to, the PI protection system of the foreign country and actions to be undertaken by the relevant third-party transferees for the protection of PI.

Also, regarding the above second exception, the 2020 Amendment has introduced that the transferor shall periodically monitor the status of implementation by the foreign third-party transferee of protective measures and any system of the foreign country that may affect the implementation measures, and take necessary and appropriate measures if the implementation of such protective measures is hindered. Upon request of affected data subjects, the transferor will also be required to provide them with information useful to the data subjects.

Law stated - 31 May 2023

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

The restrictions on the cross-border transfers of PI under the APPI are equally applicable to transfers to service providers. They may also apply to onward transfers in the sense that the initial private business operators must ensure that not only the transferors of such onward transfers but also their transferees adhere to the cross-border restrictions of the APPI.

Law stated - 31 May 2023

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

There is no statutory requirement under the APPI that data should be stored in Japan. This requirement, however, exists in certain limited industries. For instance, under the Security Guidelines for Providers of Information Systems and Services involving Medical Information, information system and service providers that process medical information are required to have these systems and services and the relevant medical information 'within the territorial jurisdiction of Japanese law'.

Law stated - 31 May 2023

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Under the Act on the Protection of Personal Information of 2003, as amended (APPI), individuals have the right to require disclosure of their personal information (PI) held by PI data owners. Specifically, upon request from individuals, PI data owners are obligated to disclose, without delay, retained personal data of the requesting individuals (the obligation of disclosure). Such disclosure, however, is exempted as a whole or in part if such disclosure would:

- prejudice the life, body, property or other interest of the individual or any third party;
- cause material impediment to the proper conduct of the business of the PI owners; or
- result in a violation of other laws.

Law stated - 31 May 2023

Other rights

Do individuals have other substantive rights?

Under the APPI, individuals have the right to require, and PI data owners are obliged to:

- correct, add or delete the retained personal data to the extent necessary for achieving the purposes of use – the

obligations of correction etc;
- discontinue the use of or erase the retained personal data if such use is or was made, or the retained personal data in question was obtained, in violation of the APPI (subject to certain exceptions) – the obligation of cessation of use, etc); and
- discontinue disclosure to third parties of retained personal data if such disclosure is or was made in violation of the APPI (subject to certain exceptions) – the obligation of cessation of third-party disclosure.

Also, PI data owners are subject to an obligation to cease disclosure of personal data to third parties if the relevant individual 'opts out' of the third-party disclosure.

In addition, as a result of the 2020 Amendment, individuals also have the right to require PI data owners to discontinue the use of or erase, or discontinue disclosure to third parties, of retained data, if the data is no longer needed, the data was divulged in a data incident or the processing of the data may result in violation of the individual's rights and interests.

Law stated - 31 May 2023

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

The APPI does not provide for individuals' statutory right to receive compensation or the private business operators' obligation to compensate individuals upon a breach of the APPI. However, under the civil code of Japan, an individual may bring a tort claim based on the violation of his or her privacy right. Breaches of the APPI by a PI data owner will be a factor as to whether or not a tortious act existed. If a tort claim is granted, not only actual damages but also emotional distress may be compensated to the extent reasonable.

Law stated - 31 May 2023

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals' right to monetary compensation is enforced through the judicial system. Concerning violations by PI data owners of the obligations to respond to individuals' requests as separately mentioned in this chapter (ie, obligations of disclosure, correction, etc, cessation of use, etc, and cessation of third-party disclosure), individuals may exercise their rights to require PI data owners to respond to such requests through the judicial system, provided that they first request the relevant PI data owners to comply with such obligations and two weeks have passed after such request was made. Separately, the Personal Information Protection Commission may recommend PI data owners to undertake measures necessary to remedy such violations if it deems it necessary to do so for the protection of individuals' rights.

Law stated - 31 May 2023

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

No.

Law stated - 31 May 2023

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

There are no binding rules applicable to the use of 'cookies' or equivalent technology under the Act on the Protection of Personal Information of 2003, as amended (APPI). Any data collected through the use of cookies is generally considered not to be personally identifiable by itself. If, however, such data can be easily linked to other information and thereby can identify a specific individual, then the data will constitute personal data subject to the APPI.

Also, the 2020 Amendment, which fully took effect on 1 April 2022, has introduced the concept of 'individual-related information'. Individual-related information means information concerning an individual that is not personal information (PI), pseudonymised information, or anonymised information for a transferor but a transferee can identify the relevant individual by linking such transferred information with the PI held by the transferee. In the context of cookies sync, if they are not personally identifiable for a transferor but are expected to be synched and used by a transferee as personal data, these cookies would constitute 'individual-related information', and the transferor must confirm that the transferee has obtained consent from the relevant individual to the collection of such data as personal data.

The recent amendment to the Telecommunications Business Act of 1984, which take effect on 16 June 2023, introduces new rules stipulating that certain business operators must ensure that certain information regarding cookies or equivalent technology is notified, or made easily accessible, to users before placing cookies or equivalent technology in the users' devices. The information required to be notified or made available includes the category of the users' information to be transferred, the names of transferees, and the purposes of use of such information.

Law stated - 31 May 2023

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

Unsolicited marketing by email is regulated principally by the Act on Regulation of Transmission of Specified Electronic Mail. Under the Act, marketing emails can be sent only to a recipient who:

- has 'opted in' to receive them;
- has provided the sender with his or her email address in writing (eg, by providing a business card);
- has a business relationship with the sender; or
- makes his or her email address available on the internet for business purposes.

Also, the Act requires the senders to allow the recipients to 'opt out'. Marketing emails sent from overseas will be subject to this Act as long as they are received in Japan.

Unsolicited telephone marketing is also regulated by different statutes. It is generally prohibited to make marketing calls to a recipient who has previously notified the caller that he or she does not wish to receive such calls.

Law stated - 31 May 2023

Targeted advertising

Are there any rules on targeted online advertising?

The APPI does not have specific rules on targeted online advertising. In addition, any data collected through the use of cookies or equivalent technology for the purpose of targeted online advertising is generally considered not to be personally identifiable by itself. If, however, such data can be easily linked to other information and can thereby identify a specific individual, the data will constitute personal data subject to the APPI, as amended.

Law stated - 31 May 2023

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

The APPI imposes stringent rules for sensitive PI, including race, beliefs, social status, medical history, disabilities, criminal records and the fact of having been a victim of a crime. Collection or disclosure under the opt-out mechanism of sensitive personal information without the consent of the relevant individual is generally prohibited.

Also, the administrative guidelines for the financial sector provide for a similar category of sensitive information. This information is considered to include trade union membership, domicile of birth and sexual orientation, in addition to sensitive PI. The collection, processing or transfer of such sensitive information by financial institutions is prohibited, even with the consent of the relevant individual, except under limited circumstances permitted under such administrative guidelines.

Law stated - 31 May 2023

Profiling

Are there any rules regarding individual profiling?

The APPI does not have specific rules on individual profiling. However, private business operators are required to specify the purposes for which the PI is used as explicitly as possible under the APPI. In this regard, the Personal Information Protection Commission (the Commission) explains in the cross-sectoral administrative guidelines for the APPI that when analysing information, such as behaviours and interests related to an individual from the information obtained from the individual, private business operators using PI databases must specify the purpose of the use to the extent that such individual can predict and assume what kind of processing will be performed.

Also, the administrative guidelines for the telecommunication sector further provide that when information equivalent to sensitive PI is generated as a result of profiling, it is recommended for private business operators in the telecommunication sector to obtain the consent of the relevant individuals in advance, and it is also recommended for such private business operators not to use such information unnecessarily for advertisement distribution without obtaining the consent of the relevant individuals.

Law stated - 31 May 2023

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

The Commission has published its stance that the use of cloud server services to store personal data does not constitute disclosure to outsourced processing service providers as long as it is ensured by contract or otherwise that the service providers are properly restricted from accessing personal data stored on their servers. If the use of a particular cloud computing service is considered to constitute disclosure to outsourced processing service providers, private business operators using PI databases are required to engage in 'necessary and appropriate' supervision over the cloud service providers to safeguard the transferred personal data. Additionally, private business operators need to confirm that the service providers, if the servers are located outside of Japan, meet the equivalency test so as not to trigger the requirement to obtain prior consent from the individuals to the cross-border transfer of data.

Also, the cross-sectoral administrative guidelines for the APPI published by the Commission elaborate that when private business operators using PI databases handle personal data in a foreign country (including storing personal data in the servers located outside of Japan), they must take necessary and appropriate measures for the security control of personal data after understanding the PI protection regime of such foreign country.

Law stated - 31 May 2023

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The Act on the Protection of Personal Information of 2003, as amended (APPI) has recently undergone several significant amendments. One of the recent significant amendments was promulgated on 12 June 2020 (the 2020 Amendment) and fully implemented on 1 April 2022. The 2020 Amendment includes, inter alia, a statutory obligation to report certain data breaches to the Personal Information Protection Commission and notify affected individuals of data breaches that are likely to cause the violation of individual rights and interests.

Another recent amendment was promulgated on 19 May 2021 (the 2021 Amendment) and fully implemented on 1 April 2023. The 2021 Amendment expanded the scope of the APPI to include rules applicable not only to private sectors but also to government sectors.

Law stated - 31 May 2023

Jurisdictions

Australia	Piper Alderman
Austria	Knyrim Trieb Rechtsanwälte
Belgium	Hunton Andrews Kurth LLP
Brazil	Mattos Filho Veiga Filho Marrey Jr e Quiroga Advogados
Canada	.
Chile	Magliona Abogados
China	Mayer Brown
France	Aramis Law Firm
Germany	Hoffmann Liebs Fritsch & Partner
Greece	GKP Law Firm
Hong Kong	Mayer Brown
Hungary	VJT & Partners
India	AP & Partners
Indonesia	SSEK Law Firm
Ireland	Walkers
Italy	ICT Legal Consulting
Japan	Nagashima Ohno & Tsunematsu
Jordan	Nsair & Partners - Lawyers
Malaysia	SKRINE
Malta	Fenech & Fenech Advocates
New Zealand	Anderson Lloyd
Pakistan	S.U.Khan Associates Corporate & Legal Consultants
Poland	Kobylanska Lewoszewski Mednis
Portugal	Morais Leitao Galvao Teles Soares da Silva and Associados
Serbia	BDK Advokati

South Africa	Covington & Burling LLP
South Korea	Bae, Kim & Lee LLC
Switzerland	Lenz & Staehelin
Taiwan	Formosa Transnational Attorneys at Law
Thailand	Formichella & Sritawat Attorneys at Law
Turkey	Turunç
United Arab Emirates	Bizilance Legal Consultants
United Kingdom	Hunton Andrews Kurth LLP
USA	Hunton Andrews Kurth LLP