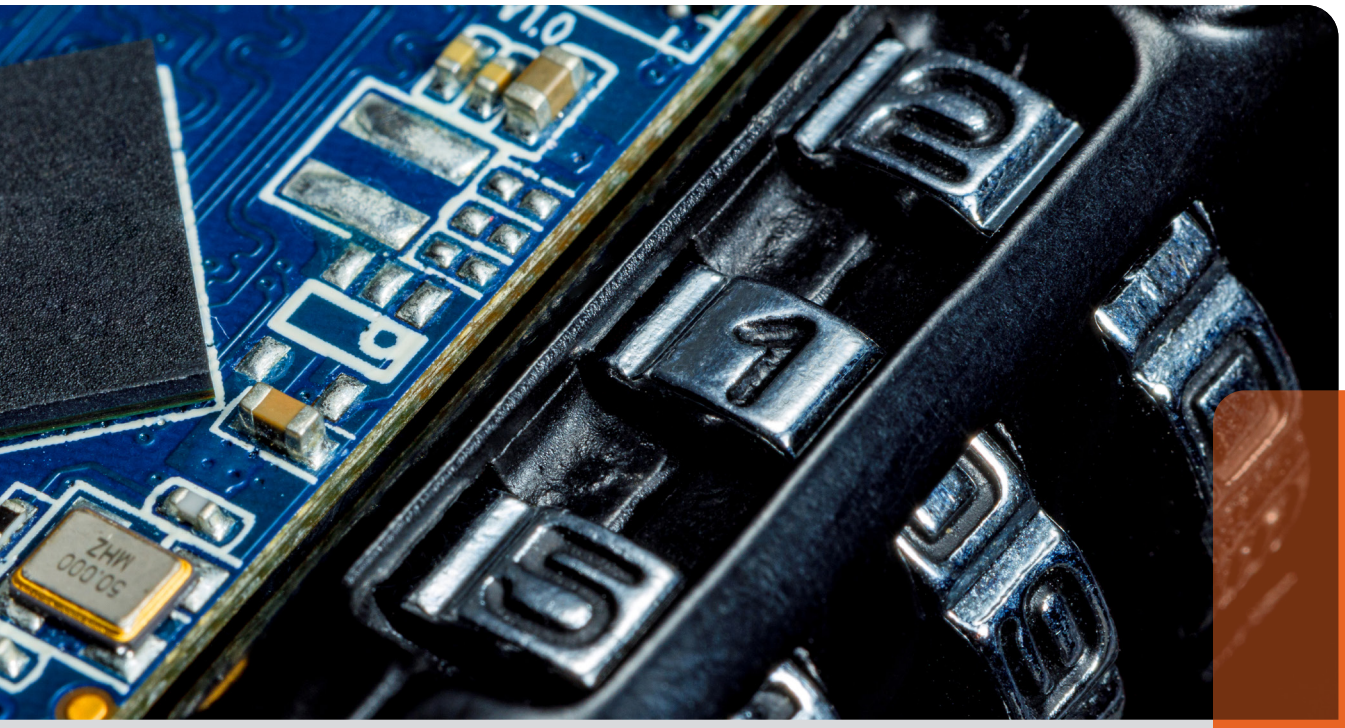
International
Comparative
Legal Guides



Data Protection

2024

11th Edition

Contributing Editors:
Tim Hickman & Detlev Gabel
White & Case LLP

glg Global Legal Group

Expert Analysis Chapters

Q&A Chapters

Japan


Hiromi Hayashi


Masaki Yukawa

Mori Hamada & Matsumoto

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Act on the Protection of Personal Information (Act No. 57 of 2003; the "**APPI**"), which applies to both the public and the private sectors.

The Personal Information Protection Committee (the "**PPC**"), which is the main agency that enforces the APPI, issues general guidelines on the implementation of the APPI. Guidelines that apply specifically to certain industries (e.g., financial, healthcare and telecommunication sectors) are jointly issued by the PPC and the competent government body that supervises the relevant industry.

APPI

It is the APPI's basic principle that the cautious handling of personal information (see question 2.1 for the definition), under the principle of respect for individuals, will promote the proper handling of personal information (APPI, Article 3).

Chapters 2 and 3 of the APPI set forth the basic frameworks of the responsibilities and policies of the national and local governments to protect personal information. Pursuant to Article 7 of the APPI, the Cabinet established the "Basic Policy on the Protection of Personal Information" (*Kojin Jyouhou no Hogo ni kansuru Kihon Houshin*) in 2004 (as amended; the "**Basic Policy**").

Chapter 4 regulates the use of personal information by private businesses and sets forth the obligations of "Business Operators Handling Personal Information" (*Kojin Joho Toriatsukai Jigyosha*) (the "handling operators"), as defined in Article 16, paragraph 2 of the APPI. Any business operator using a personal information database (please see question 2.1 for the definition) is considered a handling operator regardless of the scale of its personal information database. Chapter 4 also regulates person-related information, pseudonymised information and anonymised information (see question 2.1 for the definitions).

Chapter 5 regulates the handling of personal information by administrative organs and independent administrative agencies.

Privacy Mark

A business operator may use a logo called a "Privacy Mark" (the "**Privacy Mark System**") issued by the Japan Information Processing Development Center to certify its compliance with the relevant laws and the Japan Industrial Standards ("**JIS Q 15001**"). JIS Q 15001 is not a law; however, in certain aspects, it provides a higher level of standards than the APPI. The most updated version of JIS Q 15001 is the 2023 version and certification based on the new version is expected to be issued from October 2024.

1.2 Is there any other general legislation that impacts data protection?

(a) **Privacy right**

The right to privacy is recognised by Japanese courts as an individual's right to keep their private life private, and for their private life not to be disclosed without a legitimate reason. This is recognised among academics as the right to control one's own personal information. Therefore, in addition to complying with the APPI, a person who possesses the personal information of others in Japan must not infringe on the privacy rights of the principals.

(b) **Privacy of communications**

Article 4 of the Telecommunications Business Act provides that no person may infringe on the privacy of the communications handled by telecommunications business operators. The privacy of communications does not necessarily refer to personal information, although the guidelines issued by the Ministry of Internal Affairs and Communication ("**MIC**") for the protection of personal information in the telecommunication business (please see question 1.3) also deal with the privacy of communications, such as telecommunications logs (the "**MIC Guidelines**").

(c) **Electronic mail**

The Act on the Regulation of the Transmission of Specified Electronic Mail (Act No. 26 of 2002) regulates unsolicited marketing by email. Please see question 9.1.

(d) **Specified commercial transactions**

The Act on Specified Commercial Transactions (Act No. 57 of 1976) regulates, among other forms of unsolicited marketing, unsolicited marketing by email. Please see question 9.1.

(e) **Utilisation of numbers to identify individuals in administrative procedures**

The Japanese government adopted a social security and tax number system and, in 2015, assigned specific numbers to entities and individuals pursuant to the Act on the Utilisation of Numbers to Identify Specific Individuals in Administrative Procedures (Act No. 27 of 2013; the "**Individual Number Act**"). The collection, provision and use of the numbers assigned to individuals are allowed only for statutorily provided purposes (such as submission of tax notifications) and may not be used for other purposes.

(f) Telecommunications Business Act

The Telecommunications Business Act provides (i) requirements to protect information that can identify users (such as access log data) applicable to large-scale telecommunications service providers (please see question 1.3 and section 8), and (ii) requirements for the use of third-party cookies or otherwise transmitting information to third-party servers (please see section 11).

1.3 Is there any sector-specific legislation that impacts data protection?

The PPC was established in 2016, as the main agency that will enforce and apply the APPI. While the PPC issues general guidelines on the implementation of the APPI (the "**PPC Guidelines**"), the PPC also issued certain sector-specific guidelines jointly with other ministries, such as: (i) telecommunications sector guidelines issued jointly with the MIC; (ii) broadcasting sector guidelines issued jointly with the MIC; (iii) postal service sector guidelines issued jointly with the MIC; (iv) genetic information business guidelines issued jointly with the Ministry of Economy, Trade and Industry; (v) financial sector guidelines issued jointly with the Financial Services Agency; and (vi) medical sector guidelines issued jointly with the Ministry of Health, Labour and Welfare.

In an amendment to the Telecommunications Business Act, which took effect in June 2023, telecommunications service providers with 10 million or more users (for free-of-charge services) or 5 million or more users (for paid services) will be designated as large-scale telecommunications service providers by the MIC. If so designated, they must (i) establish information protection procedures and submit them to the MIC within three months from the designation, (ii) disclose information protection policies within three months from the designation, (iii) appoint an information protection officer and notify the MIC of the appointment within three months from the designation, (iv) annually review compliance with the said information protection procedures and policies, data breaches, and other matters regarding information protection, and (v) report certain data breaches (please see question 2.1) to the MIC.

1.4 What authority(ies) are responsible for data protection?

The PPC, as an independent regulatory body, is authorised to advise a handling operator or require it to prepare and submit a report on the handling of personal information to the extent necessary to implement the APPI (APPI, Articles 146 and 147). If a handling operator violates the APPI, the PPC may urge it to cease the violation and take other necessary measures to correct the violation (*id.* Article 148, paragraph 1). If the PPC finds it necessary and certain requirements are met, it may order the handling operator to take the urged measures or to cease the violation and take other necessary measures to rectify the violation (*id.* Article 148, paragraphs 2 and 3).

The PPC is also responsible for the supervision and enforcement of the Individual Number Act (Article 33).

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal data**"

  The APPI provides for four definitions relevant to personal data:
  - "**Personal information**" is information about living individuals that (a) can identify specific individuals, or (b) contains an "Individual Identification Code". Information that can identify specific individuals under clause (a) of the definition includes information that can be readily collated with other information to identify specific individuals.

    The "**individual identification code**" under clause (b) of the definition of "personal information" above refers to any character, number, symbol or other code (i) into which certain body features (such as DNA, appearance and fingerprints) of a specific individual has been converted by computers for use and which can identify such specific individual, or (ii) which is assigned to individuals (such as a driver's licence number, number assigned under the Individual Number Act, and passport number) (APPI, Article 2, paragraphs 1 and 2).
  - "**Personal information database**" means an assembly of information including the following: (i) an assembly of information systematically arranged in such a way that specific personal information can be retrieved by a computer; and (ii) an assembly of information designated by a Cabinet Order as being systematically arranged in such a way that specific personal information can be easily retrieved. However, any assembly of information the use of which is not likely to harm the interests of the individual principals, as further set out in the Cabinet Order of the APPI, is excluded from the definition (*id.* Article 16, paragraph 1).
  - "**Personal data**" means personal information constituting a personal information database (*id.* Article 16, paragraph 3).
  - "**Retained personal data**" means personal data that a handling operator has the authority to disclose, correct, add, erase or delete, discontinue its utilisation or discontinue its provision to a third party. However, it excludes any personal data, the existence or absence of which, would harm the life, body or property of the relevant individual or a third party, encourage or solicit illegal or unjust acts, jeopardise the safety of Japan or harm the trust of or negotiations with other countries or international organisations, or impede crime investigations or public safety (*id.* Article 16, paragraph 4).
- "**Processing**"

  The APPI does not define "processing". Although the APPI uses certain words such as handling (*toriatsukai*), collection (*shutoku*), use (*riyou*), provisions (*teikyo*) to third parties and disclosure (*kaiji*), it does not define these words.

- "**Controller**"
  Please see the definition of "processor" below.
- "**Processor**"
  The APPI does not use "controller" or "processor". However, a handling operator (*Kojin Joho Toriatsukai Jigyosha*) may be comparable to a controller or a processor in that it is subject to obligations to protect personal information. Please see question 1.1 for the definition of a handling operator. Foreign companies doing business in Japan will be regulated as handling operators if they fall within the definition.
- "**Data subject**"
  The term "principal" would be comparable to a "data subject". Article 2, paragraph 4 of the APPI defines "principal" as a specific individual identified by personal information.
- "**Sensitive personal data**"
  "Sensitive personal data" is defined in the APPI as data referring to race, creed, social status, medical history, criminal record, whether one has been a victim of crime, and other personal information which needs careful handling so as not to cause social discrimination, prejudice or other disadvantages (APPI, Article 2, paragraph 3). The Cabinet Order for the APPI provides details of what constitutes sensitive personal data, which include: physical or mental disabilities; results of medical examinations conducted by doctors or personnel who are engaged in medical services; records of medical treatment or medical advice provided based on the results of medical examinations or due to a disease, an injury or other changes in physical or mental conditions; and history related to criminal procedures such as arrest, investigation or detention.
  Under the financial sector guidelines, handling operators in the financial sector must treat not only sensitive personal data, but also labour union membership status, family origin, domicile of origin, healthcare and sex life, which are not expressly included in the foregoing scope of sensitive personal data, as sensitive personal data.
- "**Data breach**"
  "Data breach" is not a term under the APPI; however, certain designated incidents of leakage of, loss of, and damage to personal data must be reported to the PPC. Reportable incidents include: (i) actual or suspected leakage of, loss of, or damage to personal data including sensitive personal data; (ii) actual or suspected leakage of, loss of, or damage to personal data which can be abused for economic gains; (iii) actual or suspected leakage of, loss of, or damage to personal data caused by a malicious act; and (iv) actual or suspected leakage of, loss of, or damage to personal data where more than 1,000 principals are affected. Under an APPI amendment, which took effect in April 2024, an actual or suspected leakage of, loss of, or damage to personal information before it is incorporated into a database (that is, before it is considered personal data) due to a malicious act (such as information provided online is stolen before it is entered into a database) must now also be reported.
  In addition, under the Telecommunications Business Act, the data breaches that must be reported to the MIC are any leakage of information that is (i) protected by the secrecy of communication, (ii) not protected by the secrecy of communication but where more than 1,000 users are affected, or (iii) not protected by the secrecy of communication but where such information was seized by a foreign government pursuant to a foreign law.
- "**Anonymised information**"
  "Anonymised information" is defined as information obtained by removing or replacing with random descriptions certain parts of personal information such that any specific individual cannot be identified by any means and the original personal information cannot be restored (APPI, Article 2, paragraph 6). Anonymised information is not regulated as personal information since it does not identify any individual, but certain regulations apply, such as anonymising personal information in accordance with the PPC ordinance and guidelines and the prohibition against restoring personal information.
- "**Pseudonymised information**"
  "Pseudonymised information" is defined as information obtained by removing or replacing with random descriptions certain parts of personal information such that any specific individual cannot be identified unless collated with other information (APPI, Article 2, paragraph 5). Pseudonymised information may also be regulated as personal information if a removed or replaced part is retained so that a specific individual can be identified if collated with other information; however, pseudonymised information is exempted from certain regulations. For example, pseudonymised information can be used for new purposes not notified to data subjects at the time of collection even if the new purposes are not related to the original purposes. This deregulation was introduced in April 2022 to promote data economy.
- "**Person-related information**"
  "Person-related information" is defined as any information related to any living individual other than personal information, anonymised information or pseudonymised information (APPI, Article 2, paragraph 7). This definition is broad, but most practically applies to cookies, IP addresses and device IDs, which are collected at websites and applications without user logins. The regulation of person-related information was introduced in April 2022 to require the consent of principals to allow cookies or provide IP addresses and device IDs to third parties which associate those types of information with other information to identify principals.

3 Territorial and Material Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The APPI also applies to business operators outside Japan, without regard to where they were established, if they handle personal information of individuals located in Japan in connection with the provision of goods or services to individuals located in Japan (APPI, Article 171).

3.2 Do the data protection laws in your jurisdiction carve out certain processing activities from their material scope?

The APPI defines a handling operator that is subject to APPI obligations as a business operator which uses a personal information database for business. Thus, collecting or using personal information for a personal purpose is not within the scope of the APPI. Also, collecting or using personal

information for press, literary, religious or political purposes are exempted from obligations under the APPI (please see "Exceptions" in question 4.1).

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  The APPI has no provision explicitly dealing with transparency. However, handling operators are required to either publicly announce or notify the principals of the purposes of use of their personal information promptly after the collection of personal information (subject to certain exceptions) (APPI, Article 21).
  Further, the basic policy requires handling operators to establish and publicly disclose their privacy policy or privacy statement, as well as their use of service providers to handle collected personal information and the extent of the service.
- **Lawful basis for processing**
  Handling operators are prohibited from collecting personal information by deception or other wrongful means (*id.* Article 20). The PPC published an interim policy paper on 27 June 2024 (the "**2024 PPC Paper**"), which aims to propose legislative amendments. The 2024 PPC Paper proposes to define certain patterns of unlawful processing. Handling operators are also prohibited from collecting sensitive personal information without the consent of the principal except:
  (i) if required by laws and regulations;
  (ii) if necessary to protect the life, body or property of a person and it is difficult to obtain the consent of the principal;
  (iii) if necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal;
  (iv) if necessary for governmental bodies to perform their business and getting the consent of the principal will likely impede the proper performance of business;
  (v) if the handling operator is an academic research institute and the acquisition is necessary for an academic research purpose;
  (vi) if acquired from an academic research institute and the acquisition is necessary for an academic research purpose;
  (vii) for sensitive personal information that has been disclosed to the public by the principal, governmental bodies or certain parties designated by the PPC (e.g., foreign governments and international organisations);
  (viii) if the sensitive personal information is apparent from the appearance of the principal and is collected through observation or video recording (e.g., a surveillance camera records a person using a wheelchair); or
  (ix) if received from third parties as an entrustment of personal data, through a merger or other business reorganisation, or as joint use.
- **Purpose limitation**
  Handling operators are required to specify the purposes of use of personal information to the extent possible and not to use the personal information of any person, without obtaining the prior consent of that person, beyond the scope necessary to achieve the specified purpose of utilisation of personal information (*id.* Articles 17 and 18). Further, handling operators are required to endeavour to keep personal data accurate and up to date within the scope necessary to achieve the purpose of use of personal information (*id.* Article 22).
- **Data minimisation**
  The APPI has no provision on data minimisation.
- **Proportionality**
  The APPI has no provision on proportionality.
- **Retention**
  Handling operators are required to endeavour to delete personal data if it becomes unnecessary (*id.* Article 22). Further, there may be other restrictions under industry-specific guidelines. For example, the MIC Guidelines provide that telecommunication business operators must define their retention period for personal data, which must be within the period needed for the purposes of use, and must endeavour to erase personal information without delay after the expiration of the retention period (MIC Guidelines, Article 11).
- **Restriction on provision of personal data to a third party**
  A handling operator is prohibited from providing personal data to a third party without obtaining the prior consent of the principal, subject to certain exceptions (APPI, Article 27, paragraph 1), such as an "opt-out" arrangement under which the handling operator: (a) agrees to stop providing the personal data to the third party upon the demand of the principal; and (b) notifies the principal and the PPC of the following details: (i) the name, address and name of representative of the handling operator; (ii) a statement that the provision to third parties is included in the purposes of use; (iii) the items to be provided to third parties; (iv) how the personal data is collected; (v) how the personal data is provided to third parties (e.g., by publishing a book or uploading to a website through the internet); (vi) a statement that the handling operator will stop the provision if requested by the principal; (vii) how the principal can request the cessation of the data provision (e.g., telephone, email or by written means); (viii) how the personal data is updated; and (ix) when the "opt-out" arrangement starts (*id.* Article 27, paragraph 2). It should be noted that this "opt-out" arrangement is not allowed for the provision of: (a) any sensitive personal data; (b) any personal data collected in breach of the APPI; and (c) any personal data obtained through another "opt-out" arrangement. The 2024 PPC Paper proposes to impose additional requirements for "opt-out" arrangements.
- **Exceptions**
  The obligations imposed on handling operators will not apply to handling operators that fall under any of the following items and if all or part of the purpose of handling personal information is prescribed in the following applicable items (*id.* Article 57):
  (i) broadcasting institutions, newspaper publishers, communication agencies and other forms of the press (including individuals engaged in news reporting as their business); for the purpose of news reporting;
  (ii) business operators in the business of literary work; for the purpose of literary work;
  (iii) religious organisations; for the purpose of religious activities (including activities incidental thereto); or
  (iv) political organisations; for the purpose of political activities (including activities incidental thereto).
  Prior to April 2022, universities and other organisations or groups aimed at academic studies, and persons belonging to those organisations or groups, were also exempted

from the APPI to the extent that they handle personal data for the purpose of academic studies. However, due to this exemption from the APPI, academic data transfers from EEA countries to Japanese universities and other academic institutes for academic research purposes were excluded from the adequacy decision of the European Commission in January 2019. In order to enable the foregoing excluded data transfers from EEA countries, in April 2022, APPI became applicable to academic institutes for academic research purposes with regard to security measures and principals' rights. However, universities and other academic institutes continue to be exempted from the purposes of use restriction, prohibition on Sensitive Personal Information collection, and provision of personal data to third parties.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  A handling operator is required to make accessible to the principals certain information (such as the name, address and name of representative of the handling operator, the purposes of use of personal information, how principals can exercise their rights, security measures that the handling operator takes, and how the principals can bring claims) regarding retained personal data (APPI, Article 32, paragraph 1).
  Further, at a principal's request, a handling operator must notify the principal of the purposes of use of retained personal data (*id.* Article 32, paragraph 2), subject to the following exceptions:
  (i) the purposes of use are evident from the information made available to the principal by the handling operator pursuant to Article 32, paragraph 1 of the APPI;
  (ii) disclosure of the purposes of use is likely to harm the life, body, property, or other rights or interests of the principal or a third party;
  (iii) disclosure of the purposes of use is likely to harm the rights or legitimate interests of the handling operator; or
  (iv) disclosure of the purposes of use is likely to impede the handling operator's cooperation with the national or a local government.
  In addition, the handling operator is required to disclose, without delay, and upon the request of an individual, that person's Retained Personal Data, subject to certain exceptions (*id.* Article 33), subject to the following exceptions:
  (i) disclosure will likely harm the life, body, property, or other rights or interests of the person or a third party;
  (ii) disclosure will likely seriously impede the proper execution of the business of the handling operator; or
  (iii) disclosure will violate other laws and regulations.
  A principal may specify, from among a mobile communication, an email or other means of telecommunication, how the retained personal data will be disclosed to the principal. In principle, the handling operator must provide the data by the specified means; however, the handling operator may provide the data in hard copy if the specified means is excessively costly or is otherwise difficult.
  The handling operator may charge a fee for complying with a request to notify the purpose of utilisation pursuant to Article 32, or to disclose retained personal data pursuant to Article 33.
- **Right to rectification of errors**
  The principal may request the handling operator to correct, add or delete Retained Personal Data if the Retained Personal Data are not correct. The handling operator must investigate without delay and, based on the results of the investigation, correct, add or delete, as requested by the principal, the Retained Personal Data to the extent necessary to achieve the purposes of use (*id.* Article 34).
- **Right to deletion/right to be forgotten**
  As above, the principal may request the handling operator to correct, add or delete retained personal data if the retained personal data are not correct. There is no explicit legal provision on the "right to be forgotten".
- **Right to object to processing**
  The principal may request a handling operator (a) to discontinue the use of, or erase, the retained personal data, and (b) to stop providing the retained personal data to third parties if such use or disclosure is or was made, or the retained personal data in question was obtained, in violation of the APPI. The handling operator must discontinue the use of, or the provision to third parties of, or erase, retained personal data upon the request of the principal if the request has reasonable grounds (*id.* Article 35).
  In addition, the principal may request a handling operator to (a) discontinue the use of the retained personal data, and (b) stop providing the retained personal data to third parties if the handling operator ceases to have any reason to use the retained personal data, a material data breach has occurred, or the right or legitimate interest of the principal may be harmed for any other reason.
  However, these obligations will not apply if it will be excessively costly or difficult to discontinue the use of, or to erase, the retained personal data and the handling operator takes necessary alternative measures to protect the rights and interests of the principal.
- **Right to restrict processing**
  There is no "right to restrict processing" which differs from the rights stipulated above in "right to object to processing".
- **Right to data portability**
  The APPI does not grant a right to data portability. However, the MIC Guidelines require telecommunications service providers to provide information about data portability in their privacy policy.
- **Right to withdraw consent**
  There is no explicit stipulation regarding the right to withdraw consent under the APPI.
- **Right to object to marketing**
  There are no provisions explicitly setting forth objections to marketing in the APPI, but business operators must not use personal information for marketing in certain cases. Under the financial sector guidelines, a principal may request handling operators in the financial sector to stop sending marketing materials using personal information collected in connection with loans and other credit provisions. Please see question 10.1 for the restriction on e-mail marketing.
- **Right to complain to the relevant data protection authority(ies)**
  Individuals may complain to the PPC, and the PPC will conduct necessary mediation regarding a lodged complaint (*id.* Article 129(ii)).
- **Complaint to Authorised Entities for Protection of Personal Information (*Nintei Kojin Jyouhou Hogo Dantai*)**
  Authorised Entities for the Protection of Personal Information (*Nintei Kojin Jyouhou Hogo Dantai*) are entities

authorised by the PPC to handle complaints from individuals on the handling of personal information by their respective member handling operators ("**member handling operators**"). As of 12 April 2023, 44 entities have obtained such authorisation.

When an Authorised Entity for the Protection of Personal Information is requested by an individual to resolve a complaint about the handling of personal information by a member handling operator, it must promptly notify the member handling operator of the complaint and give necessary advice, investigate the circumstances pertaining to the complaint and request the member handling operator to resolve the complaint promptly. It may, if necessary, request the member handling operator to explain in writing or orally, or request it to submit relevant materials. The member handling operator may not reject such request without a justifiable ground (*id.* Article 53).

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

The APPI does not grant individuals the right to mandate non-for-profit organisations to seek remedies on their behalf or seek collective redress. However, separately from the APPI, there is a procedural law titled the Act on Special Measures Concerning Civil Court Proceedings for Collective Redress for Property Damages Incurred by Consumers, which allows certified consumer groups to seek, on behalf of consumers, collective redress for damages. Such collective redress has not been used for data breach cases since it used to be limited to the recovery of property damages and could not be used for emotional damages. However, the scope of the said Act was broadened to cover emotional damages as well in October 2023. Furthermore, the 2024 PPC Paper proposes to allow certified consumer groups to seek injunctions against handling operators.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

The APPI does not set special rules for the handling of children's personal data. With regard to consent capacity under the APPI, the PPC guidelines clarify that, if minor principals under the age of 18 are not capable of understanding the consequences of consent, the consent of a statutory representative (parent or guardian) must be obtained where the principal's consent is required under the APPI. The 2024 PPC Paper proposes to introduce special rules for children's personal data.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The APPI imposes no requirement on a handling operator to register or notify the PPC to process personal information. However, if the handling operator provides personal information to third parties without obtaining the prior consent of the principals under an "opt-out" arrangement, it is required to notify the PPC (please see question 4.1).

The PPC is also authorised to enter offices or other places, to make inquiries and investigate, and to require a handling operator to report or submit materials regarding the handling of personal information, pseudonymised information, anonymised information or person-related information, to the extent necessary to implement the APPI (*id.* Article 146). Please see question 1.4.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please see question 7.1.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Please see question 7.1.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Please see question 7.1.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

Please see question 7.1.

7.6 What are the sanctions for failure to register/notify where required?

Please see question 7.1.

7.7 What is the fee per registration/notification (if applicable)?

Please see question 7.1.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

Please see question 7.1.

7.9 Is any prior approval required from the data protection regulator?

Please see question 7.1.

7.10 Can the registration/notification be completed online?

Please see question 7.1.

7.11 Is there a publicly available list of completed registrations/notifications?

Please see question 7.1.

7.12 How long does a typical registration/notification process take?

Please see question 7.1.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The APPI has no provision mandating the appointment of a privacy or data protection officer ("**DPO**"). However, the handling operator is required to take necessary and proper measures for the prevention of leakage, loss or damage, and for other security control of personal data (APPI, Article 23). Under the PPC Guidelines, those measures should include the following:

(i) organisational security measures, such as establishing rules for handling personal data, and specifying the person responsible for supervising the handling of personal data;
(ii) human resource security measures, including the education of employees;
(iii) physical security measures, including controlling the area where personal data is handled, such as servers and offices;
(iv) technical security measures, including controlling access to personal data; and
(v) having an understanding of the relevant country's environment if data is handled outside Japan.

The PPC Guidelines indicate that appointing a person to be in charge of the handling of personal data is an example of a proper and necessary measure. The 2024 PPC Paper proposes to introduce additional measures regarding the appointment.

Separately from the APPI, as discussed in question 1.3, large-scale telecommunications service providers designated by the MIC will be required to appoint an information protection officer and notify the MIC of the appointment.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

Although a handling operator is expected to adopt the measures described in the PPC Guidelines, the failure to adopt such measures is not a direct breach of the APPI.

The failure of large-scale telecommunications service providers to appoint an information protection officer will be punishable by a fine of up to 2 million yen.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

The APPI does not offer any special protection. However, Article 27-11, Paragraph 2 of the Telecommunications Business Act provides that the opinion of the information protection officer must be respected. Also, the MIC must be informed of the dismissal of that officer.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

Since neither the APPI nor the Telecommunications Business Act requires an information protection officer to be devoted to one entity, multiple entities may appoint the same person for that position.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no requirements under the APPI. However, the Telecommunications Business Act requires that officer to have (i) management level responsibilities, and (ii) at least three years of experience in data protection or compliance or equivalent.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Please see question 8.1.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

The APPI does not require registration/notification. However, the Telecommunications Business Act requires that the MIC be notified of the appointment and dismissal of that officer.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

There is no requirement in the APPI for a DPO to be named in a public notice. However, the privacy notice must disclose the name of the director who has capacity to represent the handling operator (e.g., CEO).

There is no requirement in the Telecommunications Business Act to disclose the name of the information protection officer to the public.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

There is no concept of "processor" under the APPI (please see question 2.1). However, there is a concept of "entrustment" of the handling of personal data in which entering into an agreement is recommended.

Under Article 27, paragraph 5(i) of the APPI, if the handling operator entrusts all or part of the handling of the personal data it acquires to an individual or another entity, that individual or entity will not be considered a "third party" under Article 27, paragraph 1.

For example, if the handling operator uses third-party vendors for services, and it shares personal data with those third-party vendors for them to use on the handling operator's behalf, and not for their own use, such transfer will be deemed an "entrustment" and the restriction on the provision of personal data to a third party under Article 27 will not apply. Please note, however, that the restriction on cross-border transfers under

Article 28 still applies when entrusting personal data to a third-party service provider outside Japan (see question 12.1).

When the handling operator "entrusts" personal information, it must exercise the necessary and appropriate supervision over the entrusted person to ensure security control over the entrusted personal data. The handling operator must ensure that the entrusted person (e.g., the third-party service provider) has taken the same appropriate measures that the handling operator is required to take. The PPC Guidelines provide that "necessary and appropriate supervision" includes appropriately selecting the service provider, concluding the necessary contracts so that the security control measures based on Article 23 of the APPI (please see question 8.1) are observed by the service provider, and knowing the status of the handling of the personal data that was entrusted to the service provider.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

There is no formality requirement, but the PPC Guidelines recommend that handling operators include the agreed security measures and the reporting requirement to enable the handling operators to know the status of a service provider's handling of personal data. Under the financial sector guidelines, handling operators in the financial sector also need to include their right to supervise, audit and require reporting from the service provider, measures to prevent the leakage of personal data, the prohibition on the use of personal data for purposes other than agreed purposes, the prerequisites for subcontracting, and the responsibility of the service provider in the case of a leakage of personal data.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Unsolicited marketing by email is regulated principally by the Act on the Regulation of the Transmission of Specified Electronic Mail (Act No. 26 of 2002; the "**Anti-Spam Act**"). Pursuant to the Anti-Spam Act, marketing emails can be sent only to recipients who (i) "opted in" to receive them, (ii) provided the sender with their email address in writing (for instance, by providing a business card), (iii) have a business relationship with the sender, or (iv) make their email address available on the internet for business purposes. In addition, the Anti-Spam Act requires the senders to allow the recipients to "opt out". The Act on Specified Commercial Transactions also adopts the opt-in system for unsolicited marketing.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

The Anti-Spam Act applies not only to business-to-consumer marketing, but also to business-to-business marketing.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

Unsolicited telephone marketing regarding certain items such as financial instruments (e.g., derivatives) is restricted under different regulations. There is no national opt-out register system.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The Anti-Spam Act will apply to any entity, whether or not it has a presence in Japan, even if its marketing emails are sent from outside Japan, as long as the receiver is in Japan.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The MIC and the Consumer Affairs Agency are the authorities in charge of enforcement of the Anti-Spam Act. There have been several enforcement cases initiated by those authorities, including a recent enforcement in March 2018.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Purchasing a marketing list is not, in itself, illegal. However, the seller must obtain the consent of the principals, unless an exemption from the consent requirement applies. In addition, the seller must keep a record of certain information related to the provision of personal data for three years, and the purchaser must be informed of the name and address of the seller, the name of the seller's representative and how the seller obtained the list, and must keep a record thereof for three years (APPI, Articles 29 and 30).

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The maximum penalties under the Anti-Spam Act are one year of imprisonment or a fine of 1 million yen for an individual, and a fine of 30 million yen for the legal entity which employed that individual.

The maximum penalty for breaching the APPI is currently either imprisonment of up to one year or a fine of up to 1 million yen for individuals and 100 million yen for legal entities (APPI, Articles 178 and 184).

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

If cookies, IP addresses and device IDs are collected at a web service or application knowing the identity of users (e.g., using user registration and log-in functions of the web service or

application), they will be regulated as personal information. However, if they are collected without knowing the identity of users (e.g., user registration or log-in is not needed), they will not be regulated as personal information but may be regulated as person-related information. The collection and internal use of person-related information are not subject to any requirements under the APPI, but the provision of person-related information to third parties may be subject to a consent requirement under the APPI depending on how the data recipient will use the person-related information. If the recipient will receive the person-related information and link it to an identified user (e.g., a web service provider with a user registration feature receives cookies with certain attributes from third parties and links such cookies to its registered users), then it must obtain the consent of users and the data provider must ascertain that the consent has been obtained before the provision of person-related information.

Separately from the APPI, the Telecommunications Business Act regulates providers of (i) message exchange services, (ii) social network services and other services to which users may post information, (iii) search services, and (iv) news sites or other services that distribute information to an unspecified audience, in the use of third-party cookies or other transmissions of information to third-party servers. Those providers must (i) provide a notification or disclosure about the use of cookies, (ii) obtain users' consent, or (iii) provide an opt-out to users.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The APPI distinguishes cookies based on how the cookies are used and not on the types. However, generally speaking, first-party cookies used by only one web service provider and not intended to be shared with third parties are usually not subject to the consent requirement, but third-party cookies intended to be shared with others may be subject to the consent requirement if shared with a third party which plans to link the cookies to identified users.

Under the Telecommunications Business Act, (i) information originally transmitted by the service providers themselves (such as first-party cookies), and (ii) information absolutely necessary to provide the service (such as OS, browser or language setting) is not subject to new requirements under the recent amendment of the Telecommunications Business Act.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Since the new regulations regarding cookies under the APPI took effect only in April 2022, there have been no enforcement cases yet.

The new regulations regarding cookies under the Telecommunications Business Act took effect in June 2023. As the regulations are very new, there have been no enforcement cases to date.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

Under the APPI, an administrative fine of up to 100,000 yen may be imposed on a data recipient who falsely declares to the data provider that it has obtained the required consent.

Under the Telecommunications Business Act, as amended, a failure to comply with the requirements on transmissions of information to third parties is not directly punishable. However, the MIC may issue a remedial order and a breach of that order is punishable by a fine of up to 2 million yen.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The prior consent of the principals is required to transfer their personal data to a third party located in a foreign country (APPI, Article 28). However, the principals' prior consent to overseas transfers of their personal data is not necessary if (i) the foreign country is specified in the PPC Ordinance as having a data protection regime with a level of protection equivalent to that of Japan, or (ii) the third-party recipient has a system of data protection which meets the standards to be prescribed by the PPC Ordinance.

As of 23 January 2019, the PPC has specified the EU and the UK as having a data protection regime with a level of protection equivalent to that of Japan by the PPC Ordinances (item (i) above). As of the same date, the European Commission also adopted the adequacy decision on Japan in accordance with Article 45 of the GDPR.

The PPC issued the Supplementary Rules for Personal Data, which have been transferred from the EU and the UK by adequacy decision. By the Supplementary Rules, the handling operators are subject to stricter regulations with regard to personal data.

The PPC Ordinance also provides that with respect to item (ii), the third-party foreign recipient must either (a) provide assurance by appropriate and reasonable methodologies that it will treat the transferred personal information pursuant to the spirit of the requirements for the handling of personal information under the APPI, or (b) have been certified under a PPC-recognised international arrangement regarding its system of handling personal information (to date, the only PPC-recognised international arrangement is the APEC Cross-Border Privacy Rules System).

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Prior to April 2022, many handling operators relied on the consent of data subjects. However, due to a new requirement for handling operators to provide information about the data protection regime of the jurisdiction to which the personal data will be transferred and the data protection measures taken by the data recipients before obtaining the consent of data subjects, more operators choose to rely on the third-party foreign recipient's assurance that it will treat the transferred personal data pursuant to the spirit of the requirements on the handling of personal information under the APPI (e.g., executing a data processing agreement to comply with the APPI). A handling operator that relies on such an assurance will need to regularly monitor the data protection of the data recipient and provide data subjects with information about the data protection of the data recipient if requested by data subjects.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

There is no required notification or approval.

12.4 Do transfers of personal data to other jurisdictions require a transfer impact assessment? If conducting a transfer impact assessment is only mandatory in some circumstances, please identify those circumstances.

Article 23 of the APPI requires handling operators to take security measures in accordance with the PPC's guidelines. Section 10-7 of the PPC's Personal Information Protection Guidelines (General Rules) requires handling operators to understand the personal information protection regimes of any foreign jurisdictions where they handle personal information and to take necessary and appropriate measures considering such foreign regimes. In Japan, this required measure is not called a transfer impact assessment, but rather an external environment understanding.

12.5 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

The PPC has not issued any guidance following the decision of the Court of Justice of the EU in *Schrems II*, probably because the adequacy decision on Japan would not be affected by the court decision.

12.6 What guidance (if any) has/have the data protection authority(ies) issued in relation to the use of standard contractual/model clauses as a mechanism for international data transfers?

The PPC has not issued any guidance regarding the use of standard contractual/model clauses issued by foreign authorities. From the Japanese regulatory perspective, the PPC's Personal Information Protection Guidelines (Rules for Data Transfer to Foreign Third Parties) should be considered.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistle-Blower Protection Act (*Koueki Tsuhosha Hogo Hou*) prohibits employers from dismissing whistle-blowers. Business operators employing more than 300 employees are required to, while business operators employing 300 or fewer employees are required to endeavour to, appoint a responsible person who will receive reports, investigate and take remedial measures, and take other measures to protect whistle-blowers.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is generally permitted.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There are no registration/notification requirements for the use of CCTV under the APPI. However, the PPC clarified the requirements applicable to use of CCTV in its Q&A published in May 2023. If the use of CCTV is apparent to visitors and is used solely for the purpose of crime prevention (and not for identifying a person, marketing or other purposes), notification to visitors is not strictly required but only recommended. On the other hand, if CCTV is used for identifying a person (e.g., matching an identified person to those on a black list), the purposes of crime prevention and such identification must be notified or announced to visitors, and the PPC also recommends that additional information such as contact information and access to a website URL or a QR code for further information be posted near the CCTV.

14.2 Are there limits on the purposes for which CCTV data may be used?

In March 2023, the PPC issued a report regarding the use of CCTV to identify persons. Since such use of CCTV may cause an invasion of privacy and discrimination, the report recommends that users of CCTV consider whether that use of CCTV is absolutely necessary for crime prevention and assess whether the necessity outweighs the risks of invasion of privacy and discrimination.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

The employer has the right to monitor workplace communications in relation to work. However, a privacy issue may arise regarding private communications in the workplace. Thus, it is recommended that employers establish internal rules prohibiting the use of company PCs and email addresses for private use, and disclosing the possibility of monitoring those devices and data.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

Please see question 15.3.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There are no statutory and special requirements for notification to or consultation with trade unions/employee representatives regarding employee monitoring. However, if an employer sets up internal rules on employee monitoring, these rules will be considered company work rules and would require prior notification to or consultation with the majority union or employee representative.

15.4 Are employers entitled to process information on an employee's attendance in office (e.g., to monitor compliance with any internal return-to-office policies)?

If an employer notifies the purpose of use to the employees before collecting their attendance status, then it may collect the status and use it for the notified purposes.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

A handling operator is obligated to take necessary and proper measures to prevent leakage, loss or damage, and for other security control, of personal data (APPI, Article 23). Further, the handling operator is required to exercise necessary and appropriate supervision over its employees and service providers to ensure the security control of personal data (*id.* Articles 24 and 25). There is no concept of controllers or processors under the APPI (please see question 2.1).

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Handling operators are required to report material data breaches (please see question 2.1) to personal data to the PPC.

Further, under the financial sector guidelines (please see question 1.3), a handling operator in the financial sector must also report non-material data breaches to the Financial Services Agency.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Handling operators are required to report material data breaches relating to personal data to the affected principals unless it is difficult to make that report and an alternative measure is taken. They are also required to report material data breaches to the PPC. Under the current regulations, a preliminary report must be filed with the PPC without delay (suggested to mean three to five days under the PPC guidelines) and a final report must be filed with the PPC within 30 days (or 60 days with regard to a data breach potentially caused by a malicious act) after the data breach becomes known to the handling operators. The 2024 PPC Paper proposes to grant an exemption from the filing of preliminary reports in relatively minor cases.

16.4 What are the maximum penalties for personal data security breaches?

If a handling operator provides or misuses a personal information database for the purpose of unlawful gains, it may be subject to imprisonment of up to one year, or a fine of up to 500,000 yen (*id.* Article 179). If the breach is committed by a person who is employed by an entity, such entity will be subject to a fine of up to 100 million yen (*id.* Article 184).

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative powers**: The PPC may require a handling operator to report or submit materials regarding its handling of personal information, enter offices or other places to conduct an investigation, make inquiries and check records or other documents (*id.* Article 146), and require an authorised entity for the protection of personal information to report regarding its activities (*id.* Article 153).

(b) **Corrective powers**: The PPC may render guidance or advice to a handling operator (*id.* Article 147), recommend a handling operator cease the violation, take necessary measures to correct the violation and other necessary measures (*id.* Article 148) and order an authorised entity for the protection of personal information to take necessary measures (*id.* Article 154).

(c) **Authorisation and advisory powers**: The PPC does not have a general authorisation or advisory power, but has the authority to grant authorisation to applicant entities to become authorised entities for the protection of personal information.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions**: The PPC will enforce their investigating or corrective powers under the APPI, but do not have the authority to enforce GDPR provisions.

(e) **Non-compliance with a data protection authority**: If an order issued by the PPC is breached, an individual may be subject to imprisonment of up to one year, or a fine of up to 1 million yen (*id.* Article 178), and the legal entity employing the individual will also be subject to a fine of up to 100 million yen (*id.* Article 184). The 2024 PPC Paper proposes to introduce an administrative monetary penalty for breaches of the APPI.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

In relation to the PPC's powers stated in question 17.1 above, the PPC would have the power to issue an order to ban a particular processing activity without the need for a court order.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

In general, the PPC renders guidance in the case of a relatively less important violation, and a recommendation in the case of a more important violation. The PPC issued one order to a business entity to cease the provision of personal data.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Partly because the PPC's enforcement power was limited to rendering guidance, advice or recommendation over the handling operators outside Japan prior to April 2022, there have been limited cases in which the PPC exercised its powers against handling operators outside Japan. Following April 2022, the PPC was granted the authority to issue orders to handling operators outside Japan to take remedial measures.

18 E-discovery/Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Under the APPI, the general rule is that the handling operator cannot provide personal data to any "third party" without obtaining the prior consent of the principal, except in specified cases (Article 27, paragraph 1). These specified cases are cases where the provision of personal data is:

(i) required by laws and regulations;
(ii) necessary to protect the life, body or property of a person and it is difficult to obtain the consent of the principal;
(iii) necessary to improve public health and promote the sound nurturing of the young and it is difficult to obtain the consent of the principal;
(iv) necessary for governmental bodies to perform their business, and getting the consent of the principal will likely impede the proper performance of such business;
(v) where the handling operator is an academic research institute, necessary for publishing or teaching research results;
(vi) where the handling operator is an academic research institute, necessary to provide personal data to a third party for joint research; or
(vii) where the third-party recipient is an academic research institute, necessary for academic research purposes.

It is understood that "governmental bodies" referenced in (iv) above would be bodies of the Japanese government and not of other countries, and "laws" referenced in (i) above would not include foreign laws. If the handling operator were compelled to disclose personal information of Japanese individuals in accordance with a foreign law or by an action of a foreign governmental institution, the handling operator may be able to disclose the personal data in accordance with (ii) above; however, to avoid any risk in this regard, it is practical to obtain the prior consent of the data subjects before transferring data in response to requests from foreign law enforcement agencies.

18.2 What guidance has/have the data protection authority(ies) issued on disclosure of personal data to foreign law enforcement or governmental bodies?

There is no specific guidance by the PPC regarding the response to requests for disclosure from foreign law enforcement or governmental bodies.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

As per questions 1.1 and 1.4, the PPC, as an independent regulatory body, has the authority to enforce the APPI. The enforcement cases brought by the PPC regarding the APPI in FY 2022 (April 2022 to March 2023) were: 81 cases where the PPC required handling operators to report or submit materials regarding their handling of personal information; one case where the PPC undertook an on-site inspection; and 115 cases where the PPC rendered guidance or advice.

19.2 What "hot topics" are currently a focus for the data protection regulator?

In March 2024, the PPC issued a guidance to a large-scale chat service operator with approximately 195 million users in a case where the personal data of approximately 520,000 users was stolen through the exploitation of vulnerabilities of a service provider's computer system. The PPC attributes the case to problems of supply chain management, incident response and governance. In light of increasing and more sophisticated cyberattacks, cyber resilience will continue to be one important topic which will continue to attract the attention of the regulator and society at large.

Also, there is a legal mandate to update the APPI every three years. On 27 June 2024, the PPC published the 2024 PPC Paper regarding specific proposals to amend the APPI, which proposed amendments are subject to further discussions, but it is expected to be legislated in 2025. Themes such as the protection of minors' personal information, allowing consumer groups to file for injunctions, flexibility for data breach reporting and administrative monetary penalties are part of the discussions. Any business operator handling Japanese personal information should pay attention to further developments.

Hiromi Hayashi is a partner at Mori Hamada & Matsumoto, which she joined in 2001. She specialises in communications law and regulation and authored the Japanese section of *Telecommunication in Asia* in 2005. Her other areas of practice are international and domestic transactions, takeover bids and corporate restructuring. Hiromi was admitted to the Bar in 2001 in Japan and in 2007 in New York. She worked at Mizuho Corporate Bank from 1989 to 1994 and at Davis Polk & Wardwell in New York from 2006 to 2007.

Mori Hamada & Matsumoto
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 5220 1811
Email: hiromi.hayashi@mhm-global.com
LinkedIn: www.linkedin.com/in/hiromi-hayashi-25676384

Masaki Yukawa is a counsel at Mori Hamada & Matsumoto, which he joined in 2009. He advises on Japanese data protection issues for domestic and international technology companies, e-commerce companies and financial institutions. He was admitted to the Bar in 2009 in Japan and in 2016 in California. He is an Information Security specialist registered with the Information-technology Promotion Agency of Japan.

Mori Hamada & Matsumoto
Marunouchi Park Building, 2-6-1
Marunouchi Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6266 8764
Email: masaki.yukawa@mhm-global.com
LinkedIn: www.linkedin.com/in/masakiyukawa

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo with offices in Bangkok, Beijing, Shanghai, Singapore, Yangon, Ho Chi Minh City, Hanoi, Jakarta and New York. The firm has over 600 attorneys and a support staff of approximately 550 people, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well known in the areas of mergers and acquisitions, finance, litigation, insolvency, telecommunications, broadcasting and intellectual property, as well as domestic litigation, bankruptcy, restructuring and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions, representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise in telecommunications, broadcasting, internet, information technology and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

www.mhmjapan.com

MORI HAMADA & MATSUMOTO

International Comparative Legal Guides

The **International Comparative Legal Guide** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Data Protection 2024 includes two expert analysis chapters and 31 Q&A jurisdiction chapters covering key issues, including:

- Relevant Legislation and Competent Authorities
- Definitions
- Territorial and Material Scope
- Key Principles
- Individual Rights
- Children's Personal Data
- Registration Formalities and Prior Approval
- Appointment of a Data Protection Officer
- Appointment of Processors
- Marketing
- Cookies
- Restrictions on International Data Transfers
- Whistle-blower Hotlines
- CCTV
- Employee Monitoring
- Data Security and Data Breach
- Enforcement and Sanctions
- E-discovery/Disclosure to Foreign Law Enforcement Agencies
- Trends and Developments

The International Comparative Legal Guides are published by: glg Global Legal Group