Chambers

GLOBAL PRACTICE GUIDES

Definitive global law guides offering comparative analysis from top ranked lawyers

Data Protection & Cyber Security

Japan
Mori Hamada & Matsumoto

chambersandpartners.com

2019

JAPAN

The 'Law & Practice' sections provide easily accessible information on navigating the legal system when conducting business in the jurisdiction. Leading lawyers explain local law and practice at key transactional stages and for crucial aspects of doing business.

Contributed by Mori Hamada & Matsumoto ***Authors:*** Yoshifumi Onodera, Hiroyuki Tanaka, Rina Shimada

Law and Practice

Contributed by Mori Hamada & Matsumoto

CONTENTS

JAPAN LAW AND PRACTICE

Contributed by Mori Hamada & Matsumoto ***Authors:*** Yoshifumi Onodera, Hiroyuki Tanaka, Rina Shimada

Mori Hamada & Matsumoto is one of the largest full-service Japan headquartered law firms. A significant proportion of the firm's work is international in nature, representing clients in cross border transactions, litigation and other dispute resolution proceedings. The firm has more than 446 lawyers and 480 support staff (including patent attorneys, licensed tax accountants, advisors, legal assistants, translators and secretaries). The firm's senior lawyers include a number of highly respected practitioners and leaders from the Japanese and international legal community, including a former secretary general of the Inter-Pacific Bar Association, prominent law professors from the University of Tokyo and previous Prosecutor-Generals of the Public Prosecutors Office.
The firm also has experienced lawyers qualified from non-Japanese jurisdictions, such as the US, England and Wales, the People's Republic of China, the Philippines, India, Indonesia, Malaysia, Singapore, Myanmar and Thailand.

Authors

Yoshifumi Onodera is a partner whose practice covers IT/TMT, Data Protection and Privacy, Disputes in Information Technology Systems Development, Intellectual Property and Entertainment and Life Sciences. He is a member of the Intellectual Property Centre Committee, Japan Federation of Bar Associations and a Member of International Bar Association (IBA), Officer of the Intellectual Property and Entertainment Law Committee. He has published a number of articles in industry publications.

Hiroyuki Tanaka is of counsel and specialises in data protection, data security, IT/MTM, software litigation and intellectual property. He is a member of International Association of Privacy Professionals (IAPP) and of the Information Network Law Association. He has published a number of articles in industry publications.

Rina Shimada is an associate specialising data protection and privacy, labour law and litigation.

1. Basic National Legal Regime

1.1 Laws

The Act on the Protection of Personal Information (Act No 57 of 30 May 2003, as amended; the "APPI") is the principal data protection legislation in Japan. It provides the basic principles for the government's regulatory authority, as well as the obligations of private business operators who handle personal information (the "Handling Operator").

Another important law is the Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (the "My Number Act"), which stipulates the special rules for what is known in Japan as the Number to Identify a Specific Individual in the Administrative Procedure ("My Number"), a 12-digit individual number assigned to each resident of Japan.

The obligations of the public sector in the handling of personal information are stipulated in the Act on the Protection of Personal Information Held by Administrative Organs, the Act on the Protection of Personal Information Held by Independent Administrative Agencies, and local regulations (*jyorei*) legislated by local governments.

Further, the Personal Information Protection Commission (the "PPC") is the regulator responsible for the APPI and the My Number Act, and has published guidelines for the handling of Personal Information (the "PPC Guidelines"). For some industrial sectors, the Ministry with jurisdiction over them has published data protection guidelines for those sectors. For example, the Financial Services Agency and the PPC have jointly published data protection guidelines for the financial sectors, and the Ministry of Internal Affairs and Communications (the "MIC") has issued data protection guidelines for telecommunication business operators.

In order to understand the restrictions under the APPI, it is important to distinguish between three different terminologies: Personal Information, Personal Data and Retained Personal Data:

The APPI defines Personal Information as information about living individuals which (a) can identify specific individuals, or (b) contains an Individual Identification Code (Article 2.1).

Information which can be used to identify specific individuals includes information that can be readily collated with other information to identify specific individuals. Whether

information can be readily collated with other information for this purpose would be determined on a case-by-case basis, depending on how it is stored or handled by the Handling Operator. For example, a simple telephone number by itself is not Personal Information; however, if the Handling Operator can easily collate an individual's telephone number with the name of the individual, the telephone number will be deemed to be "Personal Information" for the Handling Operator.

An Individual Identification Code means a partial bodily feature of a specific individual that has been converted into any character, number, symbol or other code by computers for use and which can identify such specific individual, or which is assigned to services or goods provided to an individual, or is stated or electromagnetically recorded on a card or any other document issued to an individual, to identify him or her as a specific user, purchaser or recipient of the issued document (Article 2.2). The various types of Individual Identification Codes are listed in a Cabinet Order, and include driver's licence number, passport number and health insurance number. Credit card numbers and phone numbers are not Individual Identification Codes.

Personal Datameans Personal Information contained in a Personal Information Database (Article 2.6), which is a collection of information (which includes Personal Information) that is systematically organised to enable a computer or through another means to search for particular Personal Information; however, this term excludes a collection of information that a Cabinet Order indicates as having little possibility of harming an individual's rights and interests considering how that collection uses Personal Information. Examples of collections of information that are excluded from this definition include a commercially available telephone directory or a car navigation system (Article 2.4).

Retained Personal Datameans Personal Data that a Handling Operator has the authority to disclose, correct, add, or delete content from, discontinue the use of, erase, or discontinue its provision to a third party, excluding certain limited cases (Article 2.7).

1.2 Regulators

The regulator tasked with enforcing and implementing the APPI is the PPC, which has the following powers:

- The PPC may require a Handling Operator to report or submit materials regarding its handling of Personal Information, and may enter a Handling Operator's offices or other places to investigate, make inquiries and check records or other documents (Article 40).
- The PPC may provide guidance or advice to a Handling Operator (Article 41).
- The PPC may recommend that a Handling Operator cease any violation of the APPI and take other necessary measures to correct the violation (Article 42.1).
- The PPC may order a Handling Operator to take necessary measures to implement the PPC's recommendation mentioned above and to rectify certain violations of the APPI (Articles 42.2 and 42.3).

1.3 Administration Process

The PPC does not have the authority to conduct criminal investigations, and the APPI explicitly stipulates that the PPC's power to conduct onsite inspections does not include conducting criminal investigations.

It is important to note that the APPI imposes no administrative fines. Criminal sanctions may only be imposed if the Handling Operator refuses to co-operate with an investigation by the PPC, or makes any false report in response to such investigation, or violates any order given by the PPC as a part of an administrative sanction or provides to unauthorised persons or misuses Personal Information Database for unlawful gains.

1.4 Multilateral and Subnational Issues

Japan is a member of the APEC Cross-Border Privacy Rules (CBPR) System.

While local governments have enacted local regulations (*jyorei*), such regulations are applicable only to the public sector.

1.5 Major NGOs and Self-Regulatory Organisations

The PPC accredits private organisations called Accredited Personal Information Protection Organisations (*Nintei Kojin Jyouhou Hogo Dantai*) to handle and promote the protection of Personal Information of Handling Operators properly. These Accredited Personal Information Protection Organisations process complaints against Handling Operators or provide information on Handling Operators to ensure the reliability of the business of those Handling Operators and promote the protection of Personal Information. They also establish their own rules, such as company guidelines, but these rules are not legally binding.

1.6 System Characteristics

The APPI follows the OECD's eight Privacy Principles. Japan and the EU are in discussions regarding Japan's potential certification as an "adequate" country for EU data protection purposes, and the EU's certification as an "adequate foreign country" for Japan's data protection purposes. The discussions are anticipated to come to a fruitful completion in the near future.

1.7 Key Developments
The APPI was amended on 3 September 2015, and the amendments came into force on 30 May 2017. These amendments have introduced several important changes to Japan's data protection landscape, such as overseas data transfers, extraterritorial application of the APPI, expansion of the definition of Personal Information, and creation of the PPC.

1.8 Significant Pending Changes, Hot Topics and Issues
The Ordinance implementing the APPI is expected to be amended to identify the detailed conditions for the certification of a foreign country as a country with a data-protection regime with a level of protection equivalent to that of Japan, which is one of the exceptions to restrictions on overseas data transfers. Please see **4 International Considerations** for the details on overseas data transfer.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements
A Handling Operator has various obligations under the APPI, including the following:

- it has to specify and make known to the data subject the purpose of collecting his or her Personal Information (Articles 15 and 18);
- it cannot use Personal Information for any other purpose without the consent of the data subject (Article 16);
- it has to establish appropriate safeguards to protect Personal Information (Article 20);
- it cannot transfer Personal Information to another entity without the consent of the data subject, unless it meets the requirements of any of the exceptions provided by the APPI (Article 23);
- it cannot transfer Personal Information to countries that do not have sufficient data protection safeguards without the consent of the data subject (Article 24);
- it has to keep a record of the provision of Personal Information to a third party (Article 25);
- it has to disclose, correct or suspend the use of Personal Information if requested by data subjects (Articles 28-30); and
- it has to take certain measures to anonymise Personal Information (Article 36).

The APPI has some unique exceptions regarding the transfer of Personal Data.

Under the APPI, the general rule is that a Handling Operator cannot provide Personal Data to any "third party" without the prior consent of the data subject, except in the case of entrustment or joint use, as detailed below (Article 23.1).

Entrustment
Under Article 23.5.(i) of the APPI, if a Handling Operator entrusts all or part of the handling of Personal Data it acquires to an individual or another entity, that individual or entity will not be considered a "third party" under Article 23.1.

For example, if a Handling Operator uses third-party vendors of Handling Operator Services, and shares Personal Data with those vendors for them to use on the Handling Operator's behalf and not for their own use, that transfer will be deemed an "entrustment" and is not subject to data transfer restrictions.

When a 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.

Joint Use
A Handling Operator may share and jointly use Personal Data with specific individuals or entities as long as the Handling Operator notifies the data subject or it accessible for the data subject to know of [MHM: It is different from "makes sure the data subject is aware of ", because the data subject does not necessarily be aware of, but just making it "accessible" is fine.] the following information, before any information-sharing and joint use (Article 23.5(iii)):

- the fact that Personal Data will be used jointly with specific individuals or entities;
- the Personal Data to be used jointly;
- who the joint users are;
- the purpose of the joint use; and
- the name of the individual or entity responsible for the management of the Personal Data.

After notice or publication of the foregoing matters is made, the identified joint users will not be deemed "third parties" within the context of Article 23 and, therefore, the Handling Operator and the identified joint users may share and jointly use specific items of Personal Data as if they were a single entity.

Requirement for Appointment of Privacy or Data Protection Officers
The APPI has no provision mandating the appointment of a Privacy or Data Protection Officer, but a Handling Operator is required to take necessary and proper measures to prevent leakage, loss or damage of Personal Data, and to implement other security controls. Under the PPC Guidelines, those measures should include the following:

- organisational security measures, such as establishing rules for handling Personal Data, and clarifying the person responsible for supervising the handling of Personal Data;
- human resource security measures, including the education of employees;
- physical security measures, including controlling the area where Personal Data is handled, such as servers and offices; and
- technical security measures, including controlling access to Personal Data.

The PPC Guidelines indicate that appointing a person to be in charge of the handling of Personal Information is an example of proper and necessary measures. However, 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 APPI does not have the concepts of "privacy by design" or "by default", and does not require companies to conduct privacy impact analyses.

Internal or External Privacy Policies
The PPC Guidelines recommend the disclosure of a privacy policy or privacy statement.

A Handling Operator is required to make the following information regarding Retained Personal Data available to data subjects under Article 27.1 of the APPI, and the typical method to be used is an internal and external privacy policy:

- the name of the Handling Operator;
- the purposes of the use of Retained Personal Data;
- the procedures to answer requests from data subjects to disclose, correct or suspend the use of Retained Personal Information; and
- the contact information to accept complaints regarding the processing of Retained Personal Information.

The PPC Guidelines also recommended stating the following in the basic policies as the security control measures of Personal Data, and this may typically be stipulated in an internal and external privacy policy:

- the name of the Handling Operator;
- compliance with the relevant laws, regulations and guidelines;
- an explanation regarding security control measures for Personal Data; and
- contact details for complaints and questions.

It is also recommended in the PPC Guidelines to accelerate the transparency of entrustment (eg, disclosing whether entrustment is made and what kind of work is entrusted).

Requirement to Allow Data Subject Access to Data, and Right to Correct or Expunge
A data subject may request that a Handling Operator correct, add or delete Retained Personal Data; the Handling Operator must investigate without delay and, based on the result of the investigation, correct, add or delete the Retained Personal Data, as requested, to the extent necessary to achieve the purposes of use (Article 29).

Further, the data subject may request the Handling Operator to discontinue the use of or erase Retained Personal Data, and to stop providing 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 comply if the request has reasonable grounds (Article 30). However, this obligation will not apply if it will be too costly or difficult to discontinue the use of or erase the Retained Personal Data and the Handling Operator takes necessary alternative measures to protect the rights and interests of the data subject.

Use of Data Pursuant to Anonymisation, De-Identification or Pseudonymisation
The concept of Anonymously Processed Information was introduced by the recent amendments to the APPI and is defined as information obtained by processing Personal Information such that ordinary people cannot identify a specific data subject using the processed information or restore any Personal Information from the processed information (Article 2.9). This framework was introduced to promote the use of anonymously processed information by clarifying the rules, and was expected to lead to the use of big data, innovations and new businesses. However, because of the following requirements, it is not as widely utilised in practice as was expected. A Handling Operator can provide Anonymously Processed Information to third parties without the consent of the data subjects, provided that the Handling Operator:

- produces the Anonymously Processed Information in compliance with the standards set forth in an ordinance of the PPC (the "PPC Ordinance");
- takes measures for security control in compliance with the standards set forth in the PPC Ordinance to prevent leakage;
- discloses items that will be included in the Anonymously Processed Information pursuant to the PPC Ordinance;
- when it provides Anonymously Processed Information to third parties, discloses items that will be included in the Anonymously Processed Information and the medium to be used to deliver the information in compliance with the PPC Ordinance, and explicitly informs the third party recipients that the disclosed information is Anonymously Processed Information;
- does not do anything to identify the individual; and

- takes measures to secure the safe control of, and deal with complaints regarding, the handling of Anonymously Processed Information and publicly announce such measures (Article 36; and PPC Ordinance, Articles 19 to 22).

According to the PPC Guidelines, statistical information is not Anonymously Processed Information because it is not information regarding an individual and, thus, is not covered by any regulations under the APPI.

There is no definition of "injury" or "harm" under the APPI, but infringement of privacy consists of tort under Civil Code if an individual has mental burden or mental uneasiness regarding the disclosure of such information.

2.2 Sectoral Issues

The recent APPI amendments introduced "Special Care Required Personal Information" ("Sensitive Personal Information"), which is defined as Personal Information comprising a principal's race, creed, social status, medical history, criminal record, the fact of having suffered damages from crime, or other descriptions that may be prescribed by a cabinet order as requiring special care in handling so as not to cause unfair discrimination, prejudice or other disadvantages to the data subject (Article 2.3). The Handling Operator must get prior consent to obtain Sensitive Personal Information (Article 17.2) and transfer the same (opt-out consent is not allowed) (Article 23.2).

Financial data is not categorised as Sensitive Personal Information; if the information can identify an individual, the financial data will be treated as ordinary Personal Information.

Medical history, physical or mental disorders and the results of health check-ups are classified as Sensitive Personal Information.

Communications Data

A voice recording by voice telephony itself is not Personal Information, but can be considered Personal Information if it can identify the owner of the voice from its contents or with other information. Even if voice recording is not considered protected Personal Information, it is subject to protection under the basic principle of secrecy of communication granted under the Constitution of Japan and the Telecommunication Business Act (the "TBA"), which specifically protects the secrecy of telecommunication data.

The same applies to text messaging.

Internet

There is no mandatory requirement under the APPI to set up privacy policies; however, as explained above, it is common for Handling Operators who have websites to publish their privacy policy on their websites.

The use of cookies, beacons and other tracking technology is not directly regulated under the APPI, but any Personal Data collected through such technology is subject to the APPI.

Behavioural advertising is not directly regulated under the APPI, but any Personal Data collected to provide such behavioural advertising is subject to the APPI.

Video and Television

Image information in videos or television would be categorised as Personal Information and subject to restrictions under the APPI if it can identify the specific individual.

Social Media, Search Engines, Large Online Platforms

Other than the APPI, there are no special restrictions regarding data privacy specifically for social media, search engines or large online platforms. However, if those platforms are categorised as "telecommunication services" under the TBA, the provider will be subject to MIC's guidelines on Personal Information for telecommunication businesses.

Japan has no explicit legal provision on the "right to be forgotten". This issue was touched upon in a case against Google where an individual wanted his criminal record deleted from search results. The court of first instance admitted the individual's right to be forgotten and decided in favour of the individual. However, the High Court determined that there is no need to admit the claimant's "right to be forgotten" as an independent right but rather as part of the traditional discussion of privacy or defamation, and overturned the lower court's decision. On final appeal, the Supreme Court did not mention the "right to be forgotten" but denied the individual's claim because a criminal record is a matter of public interest.

Legal problems regarding hate speech have been the subject of intensive discussions of late. The Act on the Promotion of Efforts to Eliminate Unfair Discriminatory Speech and Behaviour against Persons Originating from Outside Japan was enacted in July 2016, but consists only of philosophical statements and imposes no penalty for any violation of the law.

While legal problems regarding data portability have been the subject of recent intensive discussions, no specific laws or regulations regarding data portability exist to date.

Children's Privacy

The Q&A issued by PIA explains that the consent of a minor under the age of 12-15 must be obtained from a person with parental authority over the minor.

Educational or school data is not subject to special restrictions but only to the restrictions under the APPI as Personal Information.

2.3 Online Marketing

Unsolicited marketing by email is regulated principally by the Act on the Regulation of Transmission of Specified Electronic Mail (the "Anti-Spam Act"). Under the Anti-Spam Act, marketing emails can only be sent to recipients who (i) have given prior consent to receive them, (ii) have provided the sender with their email addresses 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 Act requires the senders to allow the recipients to "opt out".

Further, the Act on Special Commercial Transactions has restrictions on marketing regarding mail order businesses, including online shopping, but does not provide for exceptions similar to items (ii) to (iv) of the preceding paragraph.

As discussed above, behavioural advertising is not directly regulated under the APPI, but any Personal Data collected to provide such behavioural advertising is subject to the APPI. There are no other specific restrictions for behavioural advertising.

There are special restrictions on telecommunication business operators regarding location information under the MIC's guidelines on Personal Information for telecommunication businesses. Under the guidelines, telecommunication business operators can obtain or transfer location information from a mobile device only with the prior consent of the data subject or if there is a justifiable cause.

2.4 Workplace Privacy

Before the amendment of the APPI in May 2017, the Ministry of Health Labour and Welfare ("MHLW") published guidelines for the handling of Personal Information related to employment. Those guidelines have been replaced by the PPC's general guidelines for the APPI.

The MHWL, however, has issued a notice regarding the health information of employees, which provides for an employer's handling of the health information of its employees, including a condition that an employer shall not handle the health information of any employee beyond the scope necessary to secure the employee's health.

Further, the Employment Security Act has special restrictions on obtaining information on job applicants during recruitment in order to prevent discrimination.

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

In principle, there is no special role for labour organisations or works councils regarding employment-related data privacy, but there is a general requirement for employers to obtain the opinion of the employee representative in establishing work rules.

The Whistleblower Protection Act prohibits employers from dismissing whistle-blowers. The Act itself does not have requirements for companies to have whistle-blower hotlines or system, but the Consumer Affairs Agency has published guidelines for private entities to establish and operate whistle-blower hotlines. The guidelines also specify several measures which companies must implement to protect the Personal Information of whistle-blowers, such as limiting persons who can access documents regarding the whistle-blowing.

2.5 Enforcement and Litigation

Administrative sanctions for violations of the APPI are as follows:

- The PPC may require a Handling Operator to report or submit materials regarding its handling of Personal Information, and enter a Handling Operator's offices or other places to investigate, make inquiries and check records or other documents (Article 40).
- The PPC may provide guidance or advice to a Handling Operator (Article 41).
- The PPC may recommend that a Handling Operator cease the violation and take other necessary measures to correct the violation (Article 42.1).
- The PPC may order a Handling Operator to take necessary measures to implement the PPC's recommendation mentioned above and to rectify certain violations of the APPI (Article 42.2 and 42.3).

Criminal sanctions for violations of the APPI are as follows:

- If a Handling Operator (natural person or a director or employee of the Handling Operator) provides a Personal Information Database to an unauthorised party or misuses a Personal Information Database for unlawful gains, it may be subject to imprisonment of up to one year, or a fine of up to JPY500,000. If the breach is committed by an employee of an entity, that entity will be subject to a fine of up to JPY500,000.

- If a Handling Operator (natural person or a director or employee of the Handling Operator) refuses to make a report or makes a false report in response to an investigation by the PPC or an administrative sanction, it may be subject to a criminal fine of up to JPY300,000. If the breach is committed by an employee of an entity, that entity will be subject to a fine of up to JPY300,000.
- If a Handling Operator (natural person or a director or employee of the Handling Operator) breaches an order of the PPC issued as part of an administrative sanction (please note that order does not include guidance, advice or recommendation by the PPC), it may be subject to imprisonment of up to six months, or a fine of up to JPY300,000. If the breach is committed by an employee of an entity, that entity will be subject to a fine of up to JPY 300,000.

The APPI does not provide the legal standards which the PPC or the prosecutors must establish to allege violations of privacy or data protection laws. However, generally, the authorities must follow the general restrictions of the Code of Criminal Procedure regarding the imposition of criminal sanctions, while the PPC does not have to follow those restrictions regarding administrative sanctions.

Publicly available information does not enable the identification of enforcement cases by the PPC since May 2017, when it became the regulator and enforcement authority of the APPI. There are some enforcement cases before the PPC became the regulator and enforcement authority of the APPI.

The data subject may go to court to seek compensation for damages or distress caused by the breach of data protection. Japanese courts recognise the right to privacy, which is the right of a person not to have his or her private life disclosed except for a legitimate reason. Article 709 of the Civil Code also provides for tort action in connection with a breach of the right to privacy.

Class Actions
The Act on Special Measures Concerning Civil Court Proceedings for Collective Redress for Property Damage Incurred by Consumers, which was enacted on 1 October 2016, allows class actions to be filed by consumers. Please note that claims allowed under that law are limited to property damage and do not cover compensation for distress caused by a breach of the APPI. However, a number of data subjects may select the same attorney-at-law to represent them, and such attorney-at-law can file one litigation for many data subjects, which can be similar to class action.

Recent Leading Cases
In a decision issued in October 2017, the Supreme Court found that the breach of a right to privacy may give rise to a claim for compensation for distress caused by the leakage of Personal Information (eg, name, birth date, address and telephone numbers). The case has been remanded to the High Court for further examination, and is still pending.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes
In criminal investigations, prosecutors and law enforcement agencies such as the police must follow the requirements of the Constitution of Japan and the Code of Criminal Procedure for any compulsory access of data. Any compulsory search or seizure can only be made with a court warrant.

In addition, the Constitution of Japan prohibits the violation of the secrecy of communication. In this regard, the Act on Wiretapping for Criminal Investigation allows investigative authorities to intercept phone conversations and electronic telecommunications only for certain serious crimes and only within the scope of a court warrant, and stipulates special restrictions for the wiretapping.

Judicial review acts as a safeguard to protect privacy.

3.2 Laws and Standards for Access to Data for National Security Purposes
Any compulsory search, seizure or wiretapping for national security purposes is also subject to the restrictions discussed above.

Judicial review acts as a safeguard to protect privacy.

3.3 Invoking a Foreign Government
Under the APPI, the general rule is that a Handling Operator cannot provide Personal Data to any "third party" without the prior consent of the data subject, except in specified cases (Article 23.1). These specified cases are where the provision of Personal Data is (1) based on laws; (2) necessary to protect the life, body or property of an individual and it is difficult to obtain the consent of the data subject; (3) especially necessary to improve public hygiene or promote the sound growth of children and it is difficult to obtain the consent of the data subject; or (4) necessary for co-operating with a state institution, a local public body or an individual or entity entrusted with executing operations prescribed by laws, and obtaining the consent of the data subject might impede the execution of those operations.

It is understood that a "state institution" referenced in clause (4) above refers only to the Japanese government and not foreign governments, and the "laws" referenced in clause (1) above do not include foreign laws.

If a Handling Operator is required to disclose Personal Data of Japanese residents in accordance with a foreign law or by the action of a foreign governmental institution, it may use exception (2) above, although this is debatable. If a Handling Operator would like to make disclosures based on foreign law or the action of a foreign government, then it is advisable that it obtains the prior consent of users to provide the user data where required by foreign law or a foreign governmental institution, through its privacy policies.

3.4 Key Privacy Issues, Conflicts and Public Debates

As discussed above, the My Number System was introduced in Japan in January 2016 to improve administrative efficiency, enhance public convenience, and enhance fairness in tax administration and social welfare in Japan. My Numbers are used by central governmental organisations and local governments for administrative procedures relating to social security, taxation and disaster response.

While there were discussions concerning the introducing of My Number, and there was, in fact, dissenting public opinion, the My Number System has now been fully implemented, and the scope of its usage is slowly expanding: from January 2018, it will be used in the financial sector, such as for getting information regarding bank saving accounts.

4. International Considerations

4.1 Restrictions on International Data Issues

There are special restrictions on the transfer of Personal Data to a foreign country. In principle, the APPI requires the transferor to obtain prior consent from individuals whose Personal Data will be transferred to a third party located in a foreign country (Article 24). Thus, the overseas transfer restrictions will apply if a foreign company transfers the user data to another company outside Japan. However, if the foreign company transfers the user data to a company in Japan, the overseas transfer restrictions will not apply. The foregoing restriction applies even in the "Entrustment" and "Joint Use" exceptions to local third-party data transfer restrictions. The data subjects' consent to overseas data transfers is not necessary unless:

- the foreign country is specified in the PPC Ordinance as a country with a data protection regime with a level of protection equivalent to that of Japan (the PPC Ordinance has not yet identified any such foreign country); or
- the third-party recipient has a system of data protection that meets the standards prescribed by the PPC Ordinance – ie, either of the following:

a) there is assurance, by appropriate and reasonable methodologies, that the recipient will treat the disclosed Personal Information in accordance with the spirit of the requirements for handling Personal Information under the APPI; or

b) the recipient has been certified under an international arrangement, recognised by the PPC, regarding its system of handling Personal Information.

The implementation of the PPC Ordinance is contained in the PPC Guidelines, under which the "appropriate and reasonable methodologies" referred to above include agreements between the disclosing party and the recipient, or inter-group privacy rules, which ensure that the recipient will treat the disclosed Personal Information in accordance with the spirit of the APPI. With respect to the second item above, the PPC Guidelines identify the APEC Cross Border Privacy Rules System (CBPRs) as a recognised international framework on the handling of Personal Information.

4.2 Government Notifications and Approvals

As discussed above, overseas data transfer restrictions do not require government notification or approval.

4.3 Data Localisation Requirements

There are no data localisation requirements under the APPI.

4.4 Sharing Technical Details

Software code or algorithms are not required to be shared with the government.

4.5 Limitations and Considerations

See **3.3 Invoking a Foreign Government**, above.

4.6 "Blocking" Statutes

There are no "blocking" statutes under Japanese law.

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

Big Data Analytics

The APPI was amended for easier utilisation of big data. Under the old APPI, the use of Personal Information beyond the scope reasonably relevant to the pre-disclosed purposes is prohibited, and the transfer of Personal Data to third parties without the consent of the data subject is, in principle, prohibited. The amended APPI introduced the concept of Anonymously Processed Information, to which the regulations regarding Personal Information will not apply. Please see **2.1 Omnibus Laws and General Requirements** for further explanation of Anonymously Processed Information.

As for big data analytics, the sharing of data will typically happen between companies subject to the contracts between those companies. The Ministry of Economy, Trade and In-

dustry (METI) has published guidelines on contracts regarding sharing (big) data between companies.

Automated Decision-Making
There are currently no laws or regulations regarding automated decision-making; however, this issue will be more important as developments in artificial intelligence continue (see below).

Profiling
There are currently no laws or regulations regarding profiling, but profiling was categorised as an issue for future discussion during the legislative process of amending the APPI.

Artificial Intelligence (Including Machine Learning)
Legal problems concerning artificial intelligence have been the subject of intensive discussions of late, including matters such as liability for actions of artificial intelligence and ownership of rights regarding contents created by artificial intelligence; however, there are no laws or regulations that target artificial intelligence at this time.

The Institute for Information and Communications Policy (IICP) and the MIC have published the "Draft AI R&D Guidelines for International Discussions", which explains the AI R&D Principles, and nine other principles for research into and the development of artificial intelligence. These are tentative guidelines for further international discussion. Some other associations regarding artificial intelligence have also published the same principles or guidelines for research into and the development of artificial intelligence.

Internet of Things (IoT)
Legal problems regarding IoT have been the subject of intensive discussions of late, but there are no specific laws or regulations targeting IoT at this time.

That said, MIC has published guidelines regarding comprehensive measures for IoT securities.

Please also refer to the sections on big data analytics and artificial intelligence.

Autonomous Decision-Making (Including Autonomous Vehicles)
Legal problems regarding autonomous vehicles, including ethical issues, disclosure of the bases and logic of autonomous decision-making processes, and responsibility for accidents have been the subject of recent intensive discussions in Japan, but there are no laws or regulations targeting autonomous vehicles at this time.

Facial Recognition
Facial recognition data is considered Personal Information and is subject to the regulations explained in the section on Privacy and Data Protection. For example, facial recognition data collected for the prevention of crimes cannot be used for marketing purposes.

Biometric Data
Biometric data is considered Personal Information and is subject to the regulations explained in the section on Privacy and Data Protection.

Geolocation
The geolocation of persons is considered Personal Information and is subject to the regulations explained in the section on Privacy and Data Protection.

Drones
There are laws and regulations on the use of drones, including the Aviation Act, prohibitions on the flight of small pilotless planes, and local government ordinances. There are also privacy concerns regarding the use of drones, and the MIC has published guidelines regarding the use on the internet of images or videos filmed by drones.

6. Cybersecurity and Data Breaches

6.1 Key Laws and Regulators
The Basic Act on Cybersecurity regulates the basic responsibility of the national government and local governments for cybersecurity (Articles 4 and 5). It also stipulates the obligation of critical information infrastructure operators (ie, operators of businesses that provide infrastructure that is the foundation of people's living conditions and economic activities, the functional failure or deterioration of which could have an enormous impact on people), cyberspace-related business providers, and research institutions such as universities (Articles 6, 7, and 8) to exert efforts to ensure cybersecurity.

Under the APPI, a Handling Operator must take necessary and appropriate action for the security control of Personal Data it handles, including preventing the leakage, loss or damage of Personal Data (Article 20). The PPC Guidelines provide examples of these measures, such as establishing and implementing basic policies, internal rules, organisational security measures, personal security measures and technical security measures.

The My Number Act provides special rules for My Numbers.

The Unfair Competition Prevention Act prohibits the infringement of trade secrets and provides for cause of actions in civil cases, such as damage compensation and injunctive relief, as well as criminal sanctions.

The Act on the Prohibition of Unauthorised Computer Access prohibits identity fraud and attacks on security holes.

The Penal Code prohibits the creation of false electronic records (Article 161-2), fraud by using computers (Article 246-2), the destruction of electronic data (Articles 258 and 259), the obstruction of a business by using computers (Article 234-2), and the creation or provision of malware (Article 168-2).

Regulators
The NISC (National Centre for Incident Readiness and Strategies for Cybersecurity) is responsible for national-level cybersecurity under the Basic Act on Cybersecurity, and publishes Cyber Security Strategies of Japan.

The National Police Agency and the Prosecutors' Office are responsible for the criminal investigation and prosecution of cybercrimes.

As stated above, the PPC is the governmental body responsible for the APPI and the My Number Act.

METI and the Information-Technology Promotion Agency of Japan have published the Cyber Security Management Guidelines (amended as of November 2017), which serve as the basic cybersecurity guidelines for companies in Japan. MIC has published comprehensive measures for the security of IoT, and the FSA has published policies for strengthening cybersecurity in the financial services sector.

The Information-technology Promotion Agency of Japan (IPA) regularly publishes important guidelines and provides information on cybersecurity. The more important guidelines include Cyber Security Management Guidelines, as explained above, guidelines for small and mid-sized companies on information security, and guidelines on preventing insider data breach. The IPA also runs the J-CSIP or the Initiative for Cyber Security Information Sharing Partnership of Japan, which shares cybersecurity information of critical information infrastructure operators.

The Japan Network Security Association (JNISA) also provides information regarding cybersecurity.

The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) acts as a "CSIRT - Computer Security Incident Response Team of CSIRTs" in the Japanese community and publishes security alerts, incident news and manuals.

6.2 Key Frameworks
Commonly deployed guidance is provided by JIS Q 27000:2014 (based on ISO/IEC27000), JIS Q 27001:2014 (based on ISO/IEC27001), and JIS Q 27002:2014 (based on ISO/IEC27002).

JIS Q 15001 is the standard that covers Personal Information and is used as the standard for issuing Privacy Mark certifications, which are common for major Japanese companies.

6.3 Legal Requirements
There is no general legal obligation to have a written information security plan or programme, but the Cyber Security Management Guidelines have provided for ten instructions, including the recognition of cybersecurity risks and the development of company-wide measures, such as drafting a data security policy. In addition, the PPC Guidelines include the implementation of a basic policy and internal rules on Personal Data as examples of security measures that should be taken for Personal Data protection.

There are no general legal obligations to draw up an incident response plan, but the Cyber Security Management Guidelines include the development of an emergency organisation framework for incidents and a recovery organisation framework to recover damages of incidents in their ten instructions. In addition, the PPC Guidelines indicate the creation of an incident response plan as an example of security measures to be taken for the protection of Personal Data.

There are no general legal obligations to appoint a Chief Information Security Officer. However, the Cyber Security Management Guidelines require the management of companies to work steadily towards putting together cybersecurity measures by giving the Chief Information Security Officer (CISO)directions on the following ten important items:

- recognising cybersecurity risks and developing company-wide measures;
- building a structure or process for cybersecurity risk management;
- securing resources (such as budget and manpower) for the implementation of cybersecurity measures;
- developing plans to deal with cybersecurity risks based on prevention of cybersecurity risks and security;
- building a system to deal with cybersecurity risks;
- implementing a cybersecurity measures' framework (PDCA);
- developing an emergency organisation framework for incidents;
- developing a recovery organisation framework to recover from damage caused by incidents;
- taking measures and monitoring the company's whole supply chain, including business partners and outsourcing companies (Article 22 of the APPI also requires a Handling Operator to supervise properly any person to whom it has entrusted the handling of Personal Data); and

- collecting and utilising information on cyber-attacks through participation in information-sharing activities, and developing the environment to utilise such information.

Under the Japanese Companies Act, the board of directors of a large company must determine the company's internal control systems, including cybersecurity management; the failure to put in place or comply with such a system may be breach of the directors' duty of due care of a prudent manager. In addition, the CISO or the director in charge of supervising the company's cybersecurity may be in breach of their duty of due care of a prudent manager if he or she does not properly take necessary actions on cybersecurity. The Cyber Security Management Guidelines stress the importance of the directors' involvement in cybersecurity management.

Although there are no general legal obligations to draw up an incident response plan, the IPA has published guidelines on how to prevent insider data breach. The Cyber Security Management Guidelines refer to the IPA's guidelines as useful guidance on minimising and dealing with insider threat.

There are no general legal obligations relating to training. However, the Cyber Security Management Guidelines include the securing of proper resources, such as setting aside adequate budget and sufficient manpower, for the implementation of cybersecurity measures in their ten instructions. In addition, the PPC Guidelines indicate that training is an example of security measures that could be taken to protect Personal Data.

6.4 Key Multinational Relationships

The Cyber Security Policy, which was issued as a Cabinet Order, emphasises the importance of multinational co-operation, especially in preventing cyber terrorism ahead of the upcoming Tokyo 2020 Olympic Games.

6.5 Key Affirmative Security Requirements

Reporting is required in relation to an investigation by the PPC for a breach of the APPI, but there is no obligation for periodic reporting to the PPC.

The fourth action plan on information security of critical infrastructure published by the Cyber Security Strategies Headquarters of the Cabinet provides for the reporting obligations of critical infrastructure service providers in the following instances:

- if there is a legal reporting requirement by the law and regulation;
- if the provider has determined that there are serious impacts to the life of people or the services of critical infrastructure and that information must be shared; or
- in other cases where the provider has determined that information must be shared.

The relevant incident and other useful information may be shared with other critical infrastructure service providers.

There are no special requirements regarding the prevention of denial of service attacks or similar attacks on system or data availability or integrity.

6.6 Data Breach Reporting and Notification

Regarding Personal Data, the PPC's Notification No. 1 (2017) defines a breach of data security as the leakage of, loss of, or damage to data. There is also a special rule for My Numbers under the My Number Act.

There are no definitions for reportable data security incidents or breaches relating to other data.

The PPC's Notification No 1 (2017) covers the following:

- leakage, loss, or damage of Personal Data held by a Handling Operator;
- leakage of a processing method for Anonymously Processed Information held by a Handling Operator; and
- possible occurrence of either of the above.

All systems are covered by the PPC's Notification No.1 (2017).

Regarding Personal Data, MHLW issues notifications on ensuring the information security of medical devices and guidelines on the security management of medical information system, but no special rule has been issued for data breach reporting and notification.

Under the PPC's Notification No 1 (2017), a Handling Operator must endeavour to report a breach to the government through the PPC, an Accredited Personal Information Protection Organisation, or any other supervising authority or organisation. However, reporting is not required in the following cases:

- the Handling Operator determines that a Personal Data leakage has not substantially occurred – for example, the Personal Data is secured by high-level encryption; or
- minor wrong transmissions of e-mail or fax or erroneous dispatch of a package – for example, the Personal Data leaked was only the name of the addressor or addressee of e-mail or the fax or package and just that email, fax or package.

The PPC's Notification No 1 (2017) provides that it is preferable for a Handling Operator to notify the data subject who may be affected by the data breach in order to prevent

further damage, and to announce publicly the fact of the data breach and the prevention measure against its recurrence, in order to prevent further damage and similar data breaches in other companies.

6.7 Ability to Monitor Networks for Cybersecurity

An employer may monitor and inspect the e-mails of its employees in connection with the implementation of its internal rule regarding e-mail monitoring, and as long as the actual e-mail monitoring is conducted only to the extent necessary. Some companies also use other digital forensic measures.

6.8 Cyberthreat Information-Sharing Arrangements

The fourth action plan on information security of critical infrastructure published by Cyber Security Strategies Headquarters of the Cabinet provides for certain reporting obligations and sharing of cybersecurity information in relation to critical infrastructure service providers, as explained above.

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

Tel: +81 3 5223 7769
Fax: +81 3 5223 7669
Email: yoshifumi.onodera@mhmjapan.com
Web: http://www.mhmjapan.com/en/firm/

MORI HAMADA & MATSUMOTO

The IPA, JNISA and JPCERT/CC accept reports or notices from the public regarding cybersecurity incidents and publish useful information.

6.9 Significant Cybersecurity, Data Breach Regulatory Enforcement and Litigation

There is no legally binding enforcement of cybersecurity measures against private companies in Japan.

Furthermore, the enforcement of the APPI regarding the protection of Personal Data is not so active: in the past 11 years, only eight official recommendations, three official advisory notices and 320 official requests for reports were made under the APPI.

No administrative order has been made regarding non-compliance with an official recommendation, and no criminal sanction for non-compliance with an order or reporting requirement has been imposed. As far as is known, the latest official recommendation was made by METI to an educational company for the leakage of Personal Information of approximately 30,000,000 data subjects. A group of data subjects has filed several civil cases in relation to this major data leak, and one shareholder of the educational company has filed a shareholder's lawsuit against the directors of the company.